# EXHIBIT A

# VERITEXT
## LEGAL SOLUTIONS

Deposition of:

## J.  Alex Halderman , Ph.D.

*February 25, 2020*

In the Matter of:

## Fair Fight Action, Inc., Et Al. Vs. Raffensperger, Brad, Et Al.

Page 1

1                    IN THE UNITED STATES DISTRICT COURT

2                    FOR THE NORTHERN DISTRICT OF GEORGIA

3                            ATLANTA DIVISION

4

5        FAIR FIGHT ACTION, et al.,

6                        Plaintiffs,

7            -vs-                    Case No. 1:18-cv-05391-SCJ

8        BRAD RAFFENSPERGER, in his

9        official capacity as Secretary

10       of State of the State of

11       Georgia, et al.,

12                        Defendants.

13       _____/

14

15

16

17           THE DEPOSITION OF J. ALEX HALDERMAN, Ph.D.

18           Taken at 31500 Wick Road

19           Romulus, Michigan

20           Commencing at 9:27 a.m.

21           Tuesday, February 25, 2020

22           Before Trisha Cameron, RDR, RMR, CRR, RPR, CSR

23

24

25

J.  Alex Halderman , Ph.D.                    February 25, 2020
Fair Fight Action, Inc., Et Al. Vs. Raffensperger, Brad, Et Al.

Page 2

1        APPEARANCES:

2        MR. ANDREW D. HERMAN

3        Miller & Chevalier

4        900 16th Street NW

5        Washington, D.C.  20006

6        (202) 626-5869

7        aherman@milchev.com

8              Appearing on behalf of the plaintiffs.

9

10       MR. BRYAN P. TYSON

11       Taylor English Duma, LLP

12       1600 Parkwood Circle, Suite 200

13       Atlanta, Georgia  30339

14       (678) 336-7249

15       btyson@taylorenglish.com

16              Appearing on behalf of the defendants.

17

18

19

20

21

22

23

24

25

J.  Alex Halderman , Ph.D.                    February 25, 2020
Fair Fight Action, Inc., Et Al. Vs. Raffensperger, Brad, Et Al.

Page 3

1                        INDEX TO EXAMINATIONS

2

3        WITNESS                                              PAGE

4        J. ALEX HALDERMAN, Ph.D.

5          EXAMINATION BY MR. TYSON                              6

6

7

8

9

10

11

12

13

14

15

16

17

18

19

20

21

22

23

24

25

J.  Alex Halderman , Ph.D.                      February 25, 2020
Fair Fight Action, Inc., Et Al. Vs. Raffensperger, Brad, Et Al.

Page 4

1                            EXHIBITS

2        DEPOSITION EXHIBIT                                    PAGE

23

24

25

J. Alex Halderman , Ph.D.                    February 25, 2020
Fair Fight Action, Inc., Et Al. Vs. Raffensperger, Brad, Et Al.

Page 5

19

20   (Exhibits attached.)

21

22

23

24

25

Page 6

1          Romulus, Michigan

2          Tuesday, February 25, 2020

3          About 9:27 a.m.

4                              *    *    *

5                         J. ALEX HALDERMAN, Ph.D.,

6                    having been first duly sworn,

7                was examined and testified as follows:

8                              *    *    *

9               MR. TYSON:   This will be the

10          deposition of Dr. Alex Halderman taken by

11          Defendant Secretary of State Brad

12          Raffensperger for the purpose of discovery

13          and all purposes allowed under the Federal

14          Rules of Civil Procedure.  And we'll

15          reserve all objections except form and

16          privilege and responsiveness until trial

17          or first use, if that's acceptable.

18               MR. HERMAN:  That's acceptable.

19                         EXAMINATION

20    BY MR. TYSON:

21    Q.   All right.  Well, good morning, Dr. Halderman.

22    A.   Good morning.

23    Q.   Brian Tyson.  We met before.  It's good to see you

24         again.

25    A.   Good to see you again too.

J. Alex Halderman , Ph.D.                    February 25, 2020
Fair Fight Action, Inc., Et Al. Vs. Raffensperger, Brad, Et Al.

Page 7

1   Q.   So I want to go over a couple ground rules just as we

2        get started today.  Have you had a chance to have

3        your deposition taken before?

4   A.   I have.

5   Q.   Okay.  And so you're going to be familiar with this.

6        For our court reporter's sake, it's best that we

7        don't talk over each other.  In conversations,

8        sometimes that's easy to do.  Sometimes you will know

9        where I'm going with a question before I get to the

10       question mark.  It's best for everybody if you can

11       wait until I get to the question mark, then answer.

12              It's best also for a yes and no, instead of

13       uh-huh and huh-uh, just because that makes for a

14       clearer better transcript.

15              And we can take breaks whenever you want to

16       along the way.  My only request is that you would

17       answer the last question I asked prior to taking a

18       break.

19              And there have been times, and it happens

20       in every deposition, where we get to the question

21       mark of a sentence, I don't know what I'm asking, you

22       don't know what I'm asking, no one is -- it's totally

23       confusing.  Let me know if that happens, and I'll

24       rephrase the question.  So will that work for you?

25  A.   Yes, I understand.

Page 8

1   Q.   Perfect.  All right.  So what I want to do is first

2        talk through some pieces of kind of how you got ready

3        for today.  Then we'll move into your background and

4        experience and then get to the report.  That's kind

5        of the general flow we'll be working with for the

6        day.

7              So what did you do to get ready for your

8        deposition today?

9   A.   So for the deposition today, I reviewed -- I reviewed

10       material that was produced by Dominion to the

11       plaintiffs that the plaintiffs provided to me that

12       was about -- that was several thousand pages of

13       documentation.  And I'm also familiar with the

14       contours of Georgia's system more generally from work

15       that I've done in the past.

16  Q.   So in terms of documents you reviewed, documents from

17       Dominion, did you review any other documents to get

18       ready for today?

19  A.   Other documents beyond what I'm generally familiar

20       with.  Let me see.  I went back and looked at

21       documentation prepared in testing the Dominion

22       equipment in California, as well as the Poll Pads in

23       California.  I reviewed certifications from

24       Pennsylvania regarding the Poll Pads and the Dominion

25       equipment, I think documentation from Texas, and a

Page 9

1        number of other resources that are cited in my

2        report.

3    Q.   Did you review any documents that are not cited in

4        your report to get ready for your deposition today?

5    A.   I don't believe so.  Not specifically for the

6        deposition today.  Perhaps the order from the Curling

7        case.  I reviewed that.

8    Q.   And that would be the 2019 order?

9    A.   Judge Totenberg's order in 2019.  That's correct.

10   Q.   Got it.  And did you talk with anybody about your

11       deposition today?

12   A.   I spoke to -- I spoke to Andrew and to Kurt, the

13       attorneys for the plaintiffs.

14   Q.   Anybody at the university who's not an attorney that

15       you spoke to?

16   A.   No.

17   Q.   Anyone else who's not one of the attorneys that you

18       talked to about your deposition today?

19   A.   No.  No.

20              (Exhibit No. 1 marked.)

21   BY MR. TYSON:

22   Q.   Okay.  I'm going to hand you what we've marked as

23       Exhibit 1, the Notice of deposition.  I'm assuming

24       you've seen that document before.

25   A.   Yes, I have.

Page 10

1   Q.   Okay.  That's just your notice.  Then what I'm going

2        to do is go ahead and mark your reports.  That way we

3        can refer to it as we're going through the

4        biographical details.  That will be easy enough on

5        that.  So I'll hand you what we've marked as Exhibit

6        2.

7                (Exhibit No. 2 marked.)

8   BY MR. TYSON:

9   Q.   I'll ask if that's the report that you filed in this

10       case.

11  A.   Yes.

12               MR. HERMAN:  Can I just note for one

13          second, this is the unsigned version.

14               MR. TYSON:  Right.  I'm going to hand

15          him --

16               (Exhibit No. 3 marked.)

17  BY MR. TYSON:

18  Q.   So I'll hand you, make it complete, what I've marked

19       as Exhibit 3.

20  A.   Yes.

21  Q.   Is that the signature page for the report that is

22       Exhibit 2?

23  A.   Yes.

24  Q.   Okay.  Wonderful.

25               MR. HERMAN:  I underestimated you.

Case 1:18-cv-05391-SCJ    Document 401-1    Filed 06/27/20    Page 13 of 243

J. Alex Halderman , Ph.D.                February 25, 2020

Fair Fight Action, Inc., Et Al. Vs. Raffensperger, Brad, Et Al.

Page 11

1              I'm sorry.

2                   MR. TYSON:   Totally fine.

3    BY MR. TYSON:

4    Q.    All right.   So, Dr. Halderman, in paragraph 13 of

5          your report, you indicate that you're being

6          compensated at a rate of $750 an hour for your work

7          on this case, correct?

8    A.    That's correct.

9    Q.    And is that -- you indicate that's your customary

10         rate.   Do you provide discounts for your expert

11         services in other cases, or is that what you charge

12         for all services?

13   A.    I generally don't provide discounts.

14   Q.    And when you say you generally don't, are there

15         specific situations where you have?

16   A.    There's -- I can think of one other situation I have

17         where work involved -- work involved a large amount

18         of rote technical work that I could do on an

19         arbitrary timeline, in which case I have.

20   Q.    And is the rate of $750 an hour generally what you

21         charge when you're working on a technical review for

22         a state or other sorts of work like that?

23   A.    Well, it depends on the circumstances.   The work that

24         I would do for a state might be anywhere from pro

25         bono to the $750 rate.

J.  Alex Halderman , Ph.D.                    February 25, 2020
Fair Fight Action, Inc., Et Al. Vs. Raffensperger, Brad, Et Al.

Page 12

1    Q.    Do you know approximately how much time you spent

2          preparing your report?

3    A.    I don't recall exactly how much time.

4    Q.    And have you sent a bill in this case?

5    A.    I haven't yet.

6    Q.    Okay.  And you plan to?

7    A.    I plan to.

8    Q.    Okay.  And you don't have a current estimate of what

9          that amount will be?

10   A.    No, I haven't prepared the bill yet.

11   Q.    All right.  So let's talk a little bit about how you

12         got involved in this lawsuit.  Did someone contact

13         you about providing a report in this litigation, or

14         how did you get started being an expert in this case?

15   A.    I was contacted by Plaintiffs' Attorneys I suppose

16         approximately a year ago.  I'd have to go back and

17         check.

18   Q.    And when you were contacted, did anyone give you

19         direction about what you were supposed to examine

20         beyond what you've described in your report?

21   A.    No, I don't believe so.

22   Q.    Did Plaintiffs' Counsel provide you with any data or

23         documents for purposes of this report?

24   A.    Yes.  They provided me with material that they --

25         that was the result of a subpoena to Dominion.

J.  Alex Halderman , Ph.D.                    February 25, 2020
Fair Fight Action, Inc., Et Al. Vs. Raffensperger, Brad, Et Al.

Page 13

1    Q.    And I should have asked.  Beyond the Dominion

2          subpoena documents, did Plaintiffs' Counsel provide

3          you any other data or documents that you relied on?

4    A.    Nothing beyond what's in the docket.

5    Q.    And did Plaintiffs' Counsel ask you to make any

6          assumptions about facts in this case for your report?

7    A.    No, they didn't.

8    Q.    Have you read the amended complaint in this case?

9    A.    Yes, I have.

10   Q.    Have you read any of the depositions that were taken

11         in this case?

12   A.    I don't believe so.

13   Q.    You indicated some docket information.  Have you read

14         any of the briefs that were filed in this case?

15   A.    I have -- I've skimmed through the docket, and I've

16         read some of the materials.  I'm not sure I've read

17         any of the briefs in full.

18   Q.    I'm not asking for your legal opinion here.  But in

19         your own words, do you have a description of what you

20         believe this case is about?

21   A.    So this case is broadly about whether election

22         practices in the state of Georgia have violated the

23         rights of Georgia voters or had discriminatory

24         effects.

25   Q.    And for your report and your work in this case,

J.  Alex Halderman , Ph.D.                    February 25, 2020
Fair Fight Action, Inc., Et Al. Vs. Raffensperger, Brad, Et Al.

Page 14

1          you're not alleging any racial component to any of

2          the problems that you've identified in your report,

3          correct?

4     A.   Well, the problems that I have discussed in my report

5          certainly could have a racial effect, especially if

6          an attacker seeking to so discord or alter the

7          outcome of an election targeted specific candidates

8          or racial groups for that effect.

9     Q.   For purposes of this report, though, you have not

10         examined any racial impacts that -- you can speculate

11         about there might be one.  But for purposes of your

12         report here, you're not alleging there are any racial

13         impacts, correct?

14    A.   I haven't gone back to examine racial data.

15    Q.   Okay.

16    A.   But certainly one of the risks, the problems that I

17         identify in this report could have is racially

18         disparate impacts.

19    Q.   And the opinions that you've authored in this report

20         in Exhibit 2 do not address the potential racial

21         impact, correct?  You're not analyzing -- let me

22         start over again.

23              The opinions you're expressing in Exhibit 2

24         are not an analysis of any racial effect of

25         particular methods of attack.  Is that a fair

Veritext Legal Solutions

J. Alex Halderman , Ph.D.                    February 25, 2020
Fair Fight Action, Inc., Et Al. Vs. Raffensperger, Brad, Et Al.

Page 15

1       statement?

2   A.  Well, they raise the possibility that -- and describe

3       methods by which an attack could occur that I think

4       it's clear could have a racial impact.  Do I analyze

5       exactly what that impact would be?  I think that

6       depends on what the attacker is hoping to achieve.

7   Q.  Maybe I can put a finer point on this.  In the

8       opinions you're expressing in your report, you're not

9       alleging that Georgia has selected particular voting

10      machines or voting practices to have a racially

11      disparate impact, are you?

12  A.  I'm not alleging intention.

13  Q.  And you're not expressing any opinion about

14      intention; is that correct?

15  A.  No, I don't go to intention.

16  Q.  As part of your work on your report, have you spoken

17      to anyone in Georgia to obtain any information that

18      you later used in your report beyond Plaintiffs'

19      Counsel?

20  A.  I have had past conversations with people in Georgia

21      that have informed my -- that have informed my

22      overall knowledge about Georgia election systems.

23  Q.  And who would those individuals be?

24  A.  I've spoken to Dr. Richard DeMillo at Georgia Tech

25      and Dr. Wenke Lee at Georgia Tech.  That's just two

Page 16

1         individuals.  And I have -- those would be probably

2         the two primary people who have informed my -- helped

3         inform my general knowledge about Georgia elections.

4    Q.   Have you spoken to any county election officials in

5         Georgia?

6    A.   No, I don't believe so.

7    Q.   Have you spoken with anyone in the Secretary of

8         State's office that resulted in information that was

9         included in your report?

10   A.   No.  But I'm generally familiar with their testimony

11        and the Curling matter and earlier litigation.

12   Q.   And when you refer to earlier litigation, beyond

13        Curling, what are you referring to there?

14   A.   Boy, all of this litigation has been going on for a

15        while, hasn't it?  I think there was -- am I correct

16        there was a state matter that -- before the Curling

17        federal matter in which there was additional

18        testimony?

19   Q.   Does Favirito versus Handel as a state court matter

20        ring a bell?  If not, that's fine.  I just thought I

21        could help identify it for you.  But if not, that's

22        fine.

23   A.   I'm sorry.

24   Q.   No problem.  Let's talk a little bit about your kind

25        of journey to here, starting with your undergraduate

J.  Alex Halderman , Ph.D.                    February 25, 2020
Fair Fight Action, Inc., Et Al. Vs. Raffensperger, Brad, Et Al.

Page 17

1          work at Princeton.  I know that you had your CV

2          attached to your report.  So I just want to walk

3          through a few questions on that.

4                  Your thesis for undergraduate work you

5          indicate was titled Investigating Security Failures

6          and Their Causes, An Analytic Approach to Computer

7          Security.

8                  Can you tell me a little bit about how you

9          arrived at that topic?  I'm sorry.  That was your

10          Ph.D. thesis.  I misspoke on that.

11    A.    How I arrived at that topic?  Can you -- what do you

12          want to know?

13    Q.    Sure.  So you focus obviously on computer security

14          and those types of issues.  How is it that you

15          arrived at wanting to study or studying this

16          particular area, cybersecurity?

17    A.    I see.  I started working on studying security

18          questions even when I was an undergrad at Princeton.

19          So you'd have to go back even farther.  But I suppose

20          what interested me most about security was that it

21          bridged both technical problems that were of

22          significant technical interest and problems involving

23          human beings and their lives, and there was an

24          opportunity in security to -- there was an

25          opportunity in security to bridge both the technical

Page 18

1          and the human elements.

2     Q.   And I know from a timing perspective we're looking at

3          kind of post-2000 election.  I'm assuming that the

4          rise in electronic voting around the same time

5          period, was that also a factor, seeing the changes in

6          the growth there?

7     A.   I'm not sure that that is what initially attracted me

8          to the security field.  I had already been working in

9          the area, but the rise of electronic voting at the

10         time was certainly one of the challenging new

11         research problems that was exciting.

12    Q.   I see you finished up in Princeton in 2009.  And then

13         where did you go from there before arriving at the

14         University of Michigan?

15    A.   I came directly to the University of Michigan.

16    Q.   Oh, I see.  I'm sorry.  I was looking at the top line

17         there.  As an assistant professor?

18    A.   That's right.

19    Q.   And so are you currently tenured at the University of

20         Michigan?

21    A.   I am.

22    Q.   And your entire academic career as a professor has

23         been at the University of Michigan, correct?

24    A.   That's correct.

25    Q.   And was there a particular item or issue that led you

J. Alex Halderman , Ph.D.                February 25, 2020
Fair Fight Action, Inc., Et Al. Vs. Raffensperger, Brad, Et Al.

Page 19

1         from Princeton to Michigan?

2    A.   Not really.  Michigan -- Michigan has a very

3         well-ranked computer science department and has one

4         of the best computing systems groups in the country,

5         which is the broader area in which most security

6         research lies.

7    Q.   And so in terms of courses that you are teaching, you

8         list some of those on there.  You've taught courses

9         on election, cybersecurity.  It's fair to say that

10        your focus really has been on cybersecurity in the

11        election context; is that a fair statement?

12   A.   That has been one of the large focuses of my work.

13        But my work is about computer security and

14        cybersecurity broadly, also work about encryption

15        technology, about securing devices attached to the

16        internet, and so on.

17   Q.   And based on the courses you have in your CV, ethics

18        is also a part of the questions you have to deal

19        with; is that correct?

20   A.   Yes.  That's correct.

21   Q.   And so in terms of kind of general principles of

22        ethical implications involved with cybersecurity

23        work, what are some topics that you cover with your

24        students on those areas?

25   A.   Questions like responsible disclosure, that is

J. Alex Halderman , Ph.D.                     February 25, 2020
Fair Fight Action, Inc., Et Al. Vs. Raffensperger, Brad, Et Al.

Page 20

1           informing manufacturers of vulnerabilities in a way

2           that helps get the vulnerabilities fixed.  Questions

3           about when is it right or lawful or not to conduct an

4           assessment of a particular system, etcetera.

5    Q.     And when you say when it's right or lawful to conduct

6           an assessment of a particular system, can you

7           elaborate on that for me real quick?

8    A.     Well, there are sometimes when there are some

9           vulnerabilities in systems that are too dangerous to

10          investigate without the cooperation of the people

11          running a system because by virtue of investigating

12          them, you might disrupt the system in a way that

13          causes broader damage.  For instance, trying to

14          without permission demonstrate ways that you could

15          hack into a hospital, which might have the effect of

16          causing people to die.  That's probably not an

17          ethical exercise in hacking.  If there are safer

18          alternatives, it would be preferred to attempt those

19          safer alternatives.

20   Q.     And then do you do any consulting or offer services

21          to companies that want you to investigate potential

22          vulnerabilities that they have?

23   A.     I have a startup company that I founded that is in

24          the business of helping companies understand the

25          vulnerabilities in their internet-facing systems.

J. Alex Halderman , Ph.D.                    February 25, 2020
Fair Fight Action, Inc., Et Al. Vs. Raffensperger, Brad, Et Al.

Page 21

1    Q.    And so I'm assuming the business model is a company

2          would retain your services through your

3          corporation -- through your company to help them

4          evaluate that?

5    A.    No.  It's not so much about retaining my services.

6          But we produce application software that helps

7          companies understand their exposure.

8    Q.    And what is the name of your company?

9    A.    It's called Censys, C-e-n-s-y-s.

10   Q.    And do you sell the software that helps companies

11         understand their exposure?

12   A.    It's kind of an annual license model.

13   Q.    And then after a company understands its exposure,

14         does Censys offer services to help it mitigate those

15         risks?

16   A.    Yes, essentially.

17   Q.    And is that more on a consulting basis as opposed to

18         the annual license model?

19   A.    No.  It's not really a consulting model.  We help to

20         point out what the vulnerabilities are and help you

21         understand which ones are important to mitigate.

22   Q.    And I'm assuming in your work with Censys and then

23         your work at the University of Michigan you never

24         encountered a system with zero vulnerabilities.  Is

25         that safe to say?

Page 22

1   A.   Yes.  I think that's probably safe to say, that

2        computing systems in general of more than trivial

3        complexity as a rule have vulnerabilities.

4   Q.   And in your work with Censys, are there situations

5        where a company is not able to mitigate all the

6        vulnerabilities you identify?

7   A.   Well, not able is a bit of a tricky statement.  So I

8        think it's a question of -- all of the

9        vulnerabilities that we identify are things that can

10       be mitigated.

11  Q.   And then it's up to the company to choose whether or

12       not they want to mitigate those vulnerabilities,

13       right?

14  A.   That's right.  Nobody forces anyone to mitigate

15       vulnerabilities in general.

16  Q.   And so ultimately, I guess maybe this is too general

17       of a statement, but there are companies that choose

18       to encounter a level of risk for some reason known to

19       them?

20  A.   Well, that's right.  And sometimes -- sometimes

21       that's clearly irresponsible.

22  Q.   Can you tell me about ISRG and what that is.

23  A.   Sure.  ISRG, the Internet Security Research Group, is

24       a not-for-profit company that I co-founded.

25  Q.   And what type of work does ISRG do?

J.  Alex Halderman , Ph.D.                    February 25, 2020
Fair Fight Action, Inc., Et Al. Vs. Raffensperger, Brad, Et Al.

Page 23

1    A.    So ISRG runs some of the critical security

2          infrastructure for the internet.  It runs a service

3          called Let's Encrypt, which is a certificate

4          authority.  That means that it vouches for the

5          identity of websites.  So if you connect to a website

6          that has https, one of the crucial steps that's going

7          on behind the scenes before you make that connection

8          is that some trusted authority has vouched for the

9          identity of the site so that your computer knows it's

10         talking to the real website and not to an attacker.

11         So ISRG and Let's Encrypt are the worlds largest

12         certificate authority.  They've issued a billion

13         certificates as of this week for several hundreds of

14         millions of websites.

15   Q.    Have you ever seen a situation where an attacker

16         attempted to appear to be a certificate authority to

17         gain access to a system.

18   A.    Yes.

19   Q.    Is that a fairly typical method of trying to attack

20         or hack a system?

21   A.    To pretend to be a certificate authority?  It's one

22         of the attacks that we as a security community spend

23         a lot of time trying to make sure it doesn't happen.

24   Q.    But it is a potential risk --

25   A.    Yes.

J. Alex Halderman , Ph.D.                    February 25, 2020
Fair Fight Action, Inc., Et Al. Vs. Raffensperger, Brad, Et Al.

Page 24

1    Q.    -- correct?  Are you paid for your services with

2          ISRG?

3    A.    No.  I only receive compensation for my travel.

4    Q.    And I'm assuming you are paid for the services Censys

5          provides, correct?

6    A.    Yes, I am.

7    Q.    So you benefit when there is a -- having visibility

8          about exposing vulnerabilities is a benefit to you as

9          advertising for Censys.  Is that fair to say?

10   A.    I suppose.  It depends on what the context of that

11         vulnerability is.

12   Q.    You indicate in your CV that in 2011 you received the

13         Election Verification Network's John Gideon Memorial

14         Award.  Do you recall that?

15   A.    Yes.

16   Q.    And what is the Election Verification Network?

17   A.    The Election Verification Network is a -- is a group

18         of election technology experts and election officials

19         and -- who are -- who work in the topic area of

20         increasing the security of elections.

21   Q.    And I'm assuming you've participated in EVN

22         conferences in the past?

23   A.    I have, yes.

24   Q.    And what does the John Gideon Memorial Award

25         recognize?

J. Alex Halderman , Ph.D.                    February 25, 2020
Fair Fight Action, Inc., Et Al. Vs. Raffensperger, Brad, Et Al.

Page 25

1   A.   I think it's scoped as recognizing contributions to

2        election integrity.

3                 (Exhibit No. 4 marked.)

4   BY MR. TYSON:

5   Q.   Dr. Halderman, I'm going to hand you what we've

6        marked as Exhibit 4.  And this is the -- appears to

7        be -- well, it's from the website of EVN for the 2019

8        conference.  And if you could turn over to the third

9        physical page.

10  A.   Page 3?

11  Q.   Yes.

12  A.   All right.

13  Q.   There's a 1:45 p.m. session on usability and voter

14       verification.  Are you with me on that?

15  A.   Yes.

16  Q.   And was this one of the panels for EVN on which you

17       appeared?

18  A.   I don't believe I appeared on that panel, no.

19  Q.   Okay.

20  A.   But I'm not listed as a panelist, and I don't recall

21       being on that panel.

22  Q.   At the -- I see your name right there.  I see Josh

23       Benaloh from Microsoft, Michelle Bishop, and then J.

24       Alex Halderman.

25  A.   Excuse me.  I was looking at the 11:45.  You mean the

Case 1:18-cv-05391-SCJ    Document 401-1    Filed 06/27/20    Page 28 of 243
J.  Alex Halderman , Ph.D.                    February 25, 2020
Fair Fight Action, Inc., Et Al. Vs. Raffensperger, Brad, Et Al.

Page 26

1       1:45 panel?

2    Q.    Got it.  My apologies.

3    A.    Yes.  That panel I did speak on.

4    Q.    And can you tell me a little bit about what usability

5          and voter verification, what topics this panel

6          covered?

7    A.    Yes.  So this panel was about -- this panel was in

8          part about ballot marking devices and the issues of

9          usability and accessibility connected to them.  It

10         was also in part about what are called end-to-end

11         verifiable voting protocols and accessibility and

12         usability attributes connected to them.

13   Q.    And maybe I can get some definitions of terms.  So

14         when you say the usability attributes of a system,

15         what is that referring to?

16   A.    It refers to -- it refers to how humans interact with

17         the technology and whether they're able to use it

18         correctly and securely.

19   Q.    And accessibility as a topic, what does that cover?

20   A.    Potential -- primarily that covers problems that may

21         involve voters or other users who have certain

22         disabilities, such as physical disabilities, and

23         their ability to use the technology.

24   Q.    And when you refer to end-to-end encryption, can you

25         describe that a little bit, please.

Page 27

1    A.    So end-to-end verifiable voting protocols are a

2          family of technologies that use advanced encryption

3          methods to provide assurance that the election

4          results were correct essentially.

5    Q.    And that's an area that's still being researched, or

6          are there products available today that provide that?

7    A.    There are products available today that provide that.

8          But it certainly is still actively being researched,

9          and there were some significant limitations to the

10         products that provide it today.

11   Q.    Let me hand you next what will be marked as Exhibit

12         5.

13               (Exhibit No. 5 marked.)

14   BY MR. TYSON:

15   Q.    And this is from the EVN website affiliated

16         organizations.  Are you aware of affiliated

17         participating organizations within EVN?

18   A.    I'm aware of some organizations that are affiliated

19         or participating, but I'm not sure that I've seen

20         this list before.

21   Q.    Okay.  And my main question, I see organizations like

22         the South Carolina Progressive Network, Common Cause,

23         the Brennan Center, the Advancement Project.  And

24         I -- my question is just going to be, do you know if

25         there are any conservative lean organizations

J.  Alex Halderman , Ph.D.                    February 25, 2020
Fair Fight Action, Inc., Et Al. Vs. Raffensperger, Brad, Et Al.

Page 28

1        affiliated with EVN?  If you don't, that's fine.

2    A.   I don't know the politics of each of these

3         organizations.  I'm sorry.

4    Q.   Easy enough.  So let's talk a little bit about the

5         expertise here.  You're an expert in cybersecurity.

6         You focused on elections, as we've talked about.

7                   Do you consider yourself an expert in

8         election administration?

9    A.   In election administration?  The subset of election

10        administration that concerns securing elections I do

11        consider myself an expert.

12   Q.   Okay.  But not in election administration broadly?

13   A.   Not in all aspects of election administration.

14   Q.   And so one of those areas within election

15        administration where you would not be an expert is

16        on, for example, best practices on chain of custody

17        for paper ballots; is that true?

18   A.   That concerns security.  So I do think I have some

19        expertise there.

20   Q.   Okay.  Which components of election administration do

21        not involve security that you would not consider

22        yourself an expert in?

23   A.   Well, I suppose not being an expert, I can't identify

24        all of the expert -- the areas that I lack expertise

25        in.

Page 29

1    Q.    Well, and the reason why I ask is in terms of

2          designing an election system, ultimately every piece

3          of design of an election system has to touch on

4          security in one way or another.  Is that fair to say?

5    A.    Probably significant amounts of the design of an

6          election system do.  I wouldn't say that every part

7          does.

8    Q.    And we have stories of, I'm sure you've heard, of

9          paper ballots being thrown into rivers, being

10         transported various methods between polling places

11         and central offices.  Do you consider yourself an

12         expert on the design of those components of handling

13         paper ballots?

14   A.    Yes, I do have expertise that's in that area.

15   Q.    And do you consider yourself an expert in the design

16         of auditing practices for elections?

17   A.    Yes.  Yes, I do.

18   Q.    Let's talk next about your testimony to congress.

19         I'll start with your most recent testimony.  You

20         testified to the House Appropriations Subcommittee on

21         Financial Service and General Government in 2019.  Do

22         you recall that testimony?

23   A.    Yes, I do.

24               (Exhibit No. 6 marked.)

25

Case 1:18-cv-05391-SCJ    Document 401-1    Filed 06/27/20    Page 32 of 243
J. Alex Halderman , Ph.D.                    February 25, 2020
Fair Fight Action, Inc., Et Al. Vs. Raffensperger, Brad, Et Al.

Page 30

1    BY MR. TYSON:

2    Q.    I'll hand you what we've marked as Exhibit 6.   I'll

3          ask if this is your written testimony for that

4          committee.

5    A.    Yes, it appears to be.

6    Q.    And almost a year ago almost to the day, not quite.

7          So --

8    A.    Has it really been only a year?

9    Q.    2019 was a long year.

10                 MR. HERMAN:   Wait until 2020.

11   BY MR. TYSON:

12   Q.    All right.   So in the second paragraph beginning

13         three years ago, you reference hackers penetrating or

14         manipulating efforts and targeting election

15         infrastructure, including voter registration systems

16         in at least 18 states.   Was Georgia one of those 18

17         states?

18   A.    Yes, it was.

19   Q.    Okay.   And so it's your testimony that hackers

20         targeted Georgia's voter registration system?

21   A.    So it's my testimony that subsequent to what I -- to

22         my written testimony from a year ago, the Senate

23         Intelligence Committee investigation has concluded

24         that the Russian -- the scope of the Russian attacks

25         was likely all 50 states, which would include

Case 1:18-cv-05391-SCJ    Document 401-1    Filed 06/27/20    Page 33 of 243
J.  Alex Halderman , Ph.D.                    February 25, 2020
Fair Fight Action, Inc., Et Al. Vs. Raffensperger, Brad, Et Al.

Page 31

1        Georgia.

2    Q.   And it's your testimony that that included Russian

3         attacks on Georgia's voter registration system, not

4         just on other components of the election system?

5    A.   I think that it's a fair inference from the findings

6         of the Senate Intelligence Committee that parts of

7         the system that are exposed to the internet like the

8         registration system were among those that the

9         Russians were targeting.

10   Q.   And when you say a system was targeted, you're not

11        necessarily saying it was accessed, correct?

12   A.   Not necessarily.

13   Q.   And not necessarily that it was manipulated in any

14        way, correct?

15   A.   Certainly not that -- you certainly can't conclude

16        from that that it was successfully manipulated.  No.

17   Q.   In the next paragraph, the end of that paragraph you

18        say, we were spared such a blow to the foundations of

19        American democracy only because Russia chose not to

20        pull the trigger.

21   A.   That's right.

22   Q.   And so would that be consistent with targeting but

23        not manipulating, that those are two different

24        things?

25   A.   So what we know is also, again, this is from the

Page 32

1          bipartisan findings of the Senate Intelligence

2          Committee, is that in one or more states, Russia had

3          the technical ability to manipulate or destroy voter

4          registration data.

5     Q.   But it's not your testimony that Russia had that

6          ability as to Georgia's voter registration system; is

7          that correct?

8     A.   Well, so it's not my testimony that the Senate

9          Intelligence Committee has concluded that Russia had

10         that ability in Georgia.  Could Russia have done that

11         in Georgia?  I think it's very likely.

12    Q.   Okay.  But you don't have any personal knowledge or

13         anything that would indicate to you that Georgia's

14         voter registration system was accessed or could have

15         been accessed by the Russians?

16    A.   Could have been accessed by the Russians?  I think

17         based on what I know about the security posture of

18         the Georgia voter registration system and about the

19         capabilities of the Russian attackers, I do think

20         it's likely that they could have accessed it.

21    Q.   Okay.  But you don't have any personal knowledge that

22         it was, in fact, accessed?

23    A.   No, I don't.

24    Q.   On the second --

25    A.   When do you think your section will be done just

Case 1:18-cv-05391-SCJ    Document 401-1    Filed 06/27/20    Page 35 of 243
J.  Alex Halderman , Ph.D.                    February 25, 2020
Fair Fight Action, Inc., Et Al. Vs. Raffensperger, Brad, Et Al.

Page 33

1        so -- I think we're getting kind of closer to an

2        hour.

3    Q.  Sure.  Maybe five, ten minutes.  Do you want to take

4        a break now?

5    A.  All right.  We'll take a break after that.  Let me

6        stretch.

7    Q.  Sure.  We can finish this document, we can do that.

8    A.  Of course.

9    Q.  So on the second physical page, you identify three

10       essential measures to protect and defend our election

11       infrastructure.  And the first you indicate is to

12       replace obsolete and vulnerable voting systems, such

13       as paperless systems with optical scanners and paper

14       ballots.

15              Are you including ballot marking device

16       systems in that as an option that we should look to

17       move to or exclusively hand-marked paper ballots?

18   A.  Ballot marking devices are important in any system

19       that uses paper ballots in order to provide an

20       independent accessible voting option for voters with

21       disabilities.  But crucially, the risk of using

22       ballot marking devices becomes very substantial when

23       they're used for all voters, as Georgia does, as

24       opposed to just for voters who request them, for

25       instance, a smaller fraction of voters.

J.  Alex Halderman , Ph.D.                     February 25, 2020
Fair Fight Action, Inc., Et Al. Vs. Raffensperger, Brad, Et Al.

Page 34

1    Q.    Would you say it's better from a security standpoint

2          for a state to replace a paperless system with a

3          system that involves at least some paper?

4    A.    Depends what they do with that paper.  If they don't

5          look at that paper or they're not looking at enough

6          of that paper, then the paper isn't serving the

7          purpose.

8    Q.    And that's true of a hand-marked paper ballot system

9          or a ballot marking device system, correct?

10   A.    If they don't look at it, that's right.  It's that

11         the paper isn't serving a purpose.

12   Q.    And which leads us to the second piece there,

13         advocating looking at the paper.  And you advocate

14         what's best -- what's known as a risk-limiting audit;

15         is that correct?

16   A.    Yes.  I recommend RLAs.

17   Q.    So an RLA, you recommend that whether a state is

18         using hand-marked ballots or ballot marking device

19         ballots, correct?

20   A.    Yes, I do.

21   Q.    On the next page, page 3, you point out that paper

22         ballots, manual audits, and security best practices

23         are endorsed by a lot of folks, including the

24         National Academies of Science, Engineering, and

25         Medicine.  I know we had this discussion previously.

Case 1:18-cv-05391-SCJ    Document 401-1    Filed 06/27/20    Page 37 of 243
J. Alex Halderman , Ph.D.                    February 25, 2020
Fair Fight Action, Inc., Et Al. Vs. Raffensperger, Brad, Et Al.

Page 35

1       But you disagree with the National Academy of

2       Sciences as to ballot marking devices; is that right?

3    A.   No, I wouldn't say that I disagree.  The National

4       Academies' report called specifically for further

5       research.  And to the question of validation on voter

6       verification of ballot marking devices and ballots

7       that they produce, substantial subsequent research,

8       including research that my own group has conducted,

9       has led to further understanding of the security

10       risks of ballot marking devices.

11   Q.   At this point, the National Academy of Sciences has

12       not changed its recommendation recommending that

13       states use either hand-marked paper ballots or ballot

14       marking devices, correct?

15   A.   I believe they'd have to go through a new consensus

16       report process in order to change what they've

17       written, and that's a process that hasn't happened

18       yet.

19   Q.   So that's a no, they haven't changed their

20       recommendation yet?

21   A.   They have not changed the published report.  They

22       haven't released the new recommendation.

23   Q.   Down at the bottom of page 3, you indicate that many

24       states would like to replace vulnerable and obsolete

25       equipment, but they are struggling to figure out how

Page 36

1       to pay for it.  So you would agree with me that there

2       are a lot of considerations for states in looking at

3       replacing voting equipment, including financial,

4       correct?

5    A.   Yes.

6    Q.   Then on the bottom of page 4, you refer to

7       voter-verifiable paper audit trails, VVPATs.

8    A.   Yes.

9    Q.   And you indicate those are badly inferior to paper

10      ballots.  Are they inferior to ballot marking device

11      paper ballots as well?

12   A.   Let me see what I've written here.  Excuse me just a

13      minute.

14   Q.   Take your time.

15   A.   So VVPATs are inferior to certain kinds of ballot

16      marking device ballots, but they do share some of the

17      problems of ballot marking device ballots.

18   Q.   I'm assuming that VVPATs and ballot marking device

19      ballots, they are both superior to paperless DREs?

20   A.   When combined with rigorous audits, they're both an

21      improvement.  The limitation is -- one of the key

22      limitations has to do with particularly close

23      elections and whether the verifiable paper trail in

24      either case accurately reflects voters' intentions.

25   Q.   Okay.  All right.  That's all I have for that

Case 1:18-cv-05391-SCJ    Document 401-1    Filed 06/27/20    Page 39 of 243
J. Alex Halderman , Ph.D.                February 25, 2020
Fair Fight Action, Inc., Et Al. Vs. Raffensperger, Brad, Et Al.

Page 37

1        exhibit.  So we can go ahead and take a break for a

2        few minutes.

3   A.   Okay.

4                  (Recess taken.)

5   BY MR. TYSON:

6   Q.   Dr. Halderman, next I want us to talk about your

7        testimony to the Senate Intelligence Committee in

8        2017.  How were you invited to attend the US Senate

9        Intelligence Committee, if you recall?

10  A.   How was I invited?  One of the -- one of the

11       committee staffers e-mailed me and invited me to

12       testify.

13                  (Exhibit No. 7 marked.)

14  BY MR. TYSON:

15  Q.   I'm going to hand you what we've marked as Exhibit 7.

16       Is that your statement to the Senate Select Committee

17       on Intelligence?

18  A.   This is my written statement.

19  Q.   If you could turn with me to page 2.  You talk about

20       in the second paragraph that optical scanners and DRE

21       voting machines are computers.  Then the third

22       sentence you say, fundamentally, they suffer from

23       security weaknesses similar to those of other

24       computer devices.

25                  You'd agree that anything that is a

Page 38

1        computer has possible security vulnerabilities?

2    A.   Yes, in general.

3    Q.   And I think, as we talked about earlier, that's true

4         of any computer.  There's going to be some

5         vulnerability that a dedicated researcher could find.

6         Fair to say?

7    A.   Yes, that's fair to say.  That's why there's some

8         applications in which we shouldn't blindly trust

9         computers to function correctly.

10   Q.   And you mention optical scanners in this group.  Is

11        that why you advocate for audits even for hand-marked

12        paper ballots counted by optical scanners?

13   A.   Yes.  Essentially that because optical scanners can

14        be hacked so that they count incorrectly, it's

15        important to verify that the election outcome is

16        correct through physical inspection of the records

17        that match the voters' intent.

18   Q.   On the third page, first full paragraph, you mention

19        that vulnerabilities are endemic throughout our

20        election system.

21             If a jurisdiction was using exclusively

22        DREs and then moved to a hand-marked paper ballot

23        system counted by optical scanners but did not

24        utilize any audits whatsoever, would you consider

25        that more or less secure as an environment?

Page 39

1    A.    But did not utilize any audits.  I would characterize

2          it as a small improvement, although still a

3          significant security risk, such as such a system

4          could withstand, for instance, the total sabotage of

5          the optical scanners and still produce an election

6          result.

7    Q.    But it could not withstand a hacking of the optical

8          scanners that was never discovered because there were

9          no audits, correct?

10   A.    That's correct.

11   Q.    If you could turn with me to page 5.  The very top of

12         page 5 and then the first full paragraph on page 5

13         discuss the Russians being in a position to sabotage

14         equipment causing the failure of voting machines,

15         resulting in long lines, and then putting the

16         Russians in a position to spread an attack and

17         potentially steal votes.

18               Is there any evidence that the scenarios

19         outlined in those first two paragraphs on page 5

20         occurred in an election?

21   A.    There is evidence that Russia did attack one or more

22         vendors of election technology and attempt to spread

23         from there to the systems of municipalities.  There

24         is -- I think it's a remaining question whether they

25         got any farther than that.

Case 1:18-cv-05391-SCJ    Document 401-1    Filed 06/27/20    Page 42 of 243

J. Alex Halderman , Ph.D.                    February 25, 2020

Fair Fight Action, Inc., Et Al. Vs. Raffensperger, Brad, Et Al.

Page 40

1    Q.   And so is there any evidence that the Russians have

2         sabotaged equipment on election day?

3    A.   So there are failures of equipment on election day

4         that there is I think it's fair to say substantial

5         question whether that failure is the result of an

6         attack or just of other forms of human error.

7    Q.   But sitting here today, you don't have any evidence

8         that equipment failure on election day was caused by

9         a Russian attack, correct?

10   A.   How would we have evidence one way or another?

11        most -- there have been few or no examinations of

12        polling place equipment since 2016 that would reveal

13        one way or another conclusively whether attacks had

14        been successful.

15   Q.   So let me ask again.  So sitting here today, you

16        don't have any evidence that any failure of equipment

17        on election day was caused by Russians, correct?

18   A.   No.  I cannot say that with high certainty that

19        failures were caused by Russia.

20   Q.   And you're not testifying to the Senate Intelligence

21        Committee or in your report here that -- I should

22        strike that.  Let me go to the next one.

23              And you don't have any evidence sitting

24        here today that the Russians have stolen votes as a

25        result of an attack on voting machines, correct?

J.  Alex Halderman , Ph.D.                    February 25, 2020
Fair Fight Action, Inc., Et Al. Vs. Raffensperger, Brad, Et Al.

Page 41

1   A.   No, there is no evidence to my knowledge that that

2        did take place.  It's -- the problem is that there

3        was nothing technical stopping that from taking place

4        in certain jurisdictions.

5   Q.   But as we discussed in your prior testimony, just

6        because you have the ability to aim the gun doesn't

7        mean you're going to pull the trigger, correct?

8   A.   No, that's right.  As I say, Vladimir Putin

9        apparently decided not to pull the trigger, and

10       that's what stopped massive chaos in 2016.

11  Q.   And in the third full paragraph on page 5 you say you

12       don't know how far the Russians got in their effort

13       to penetrate our election infrastructure, nor whether

14       they interfered with equipment on election day.  And

15       sitting here today, you still don't know how far they

16       got, correct?

17  A.   Unfortunately, that is correct.  There are still

18       large areas of election infrastructure that have not

19       been -- that have not been analyzed since 2016 in a

20       way that would allow us to know.  We may never know

21       how far the Russians got.

22  Q.   On page 6 you're reiterating the points of what you

23       recommend for safeguarding elections, and this

24       testimony obviously is in 2017.  So in the first

25       bullet when you advocate optical scanners and paper

Page 42

 1        ballots, at this time in 2017, were you also

 2        including ballot marking devices for all voters or

 3        only for those with disabilities?

 4   A.   I don't say one way or another in this testimony.

 5        And I think that at that time, I still would have

 6        said the safer thing to do is to limit the use of

 7        ballot marking devices to less than all voters.

 8   Q.   Have you had a change of your view of ballot marking

 9        devices between 2016 and today based on the research

10        you've conducted, or have you always taken the

11        position that ballot marking devices for less than

12        all voters is the best system?

13   A.   I think that my view has gone from one of the

14        conservative positions that ballot marking devices

15        are less safe than hand-marking to one that is the

16        strong research supported conclusion is that ballot

17        marking devices are far less safe.  But I think -- I

18        think at the time that this was written back in 2017,

19        I would have acknowledged that we don't yet have

20        enough evidence to conclude strongly one way or the

21        other about ballot marking devices.

22   Q.   In your CV, you also reference five congressional

23        briefings between May 2017 and September 2019.  What

24        did those briefings involve?

25   A.   Those briefings involved generally public meetings on

J. Alex Halderman , Ph.D.                    February 25, 2020
Fair Fight Action, Inc., Et Al. Vs. Raffensperger, Brad, Et Al.

Page 43

1          Capital Hill somewhere in which I tried to educate

2          members of congress and their staff about some of the

3          security risks involved in elections.

4    Q.    And were those briefings focused on the

5          vulnerabilities inherent in DREs, or did you discuss

6          other topics related to election security?

7    A.    I discussed other topics too.

8    Q.    And do you recall what those other topics would have

9          been?

10   A.    Well, in general, the threats of -- threats of

11         tampering with other kinds of voting machines, like

12         optical scanners or ballot marking devices.  They

13         would have covered risks in other components of the

14         election infrastructure like registration or

15         reporting.

16   Q.    Have you reviewed the Senate Intelligence Committee's

17         report on Russia specifically involving the efforts

18         to interfere with election infrastructure?

19   A.    Yes.

20   Q.    I'm going to hand you what we've marked as Exhibit 8.

21              (Exhibit No. 8 marked.)

22   BY MR. TYSON:

23   Q.    And I'll ask is this a report from the Senate

24         Intelligence Committee that you have reviewed

25         previously?

Page 44

1  A.  Yes, I have reviewed this.

2  Q.  I just want to ask a few questions, kind of walk

3      through this.  If you could turn first to page 3.

4      Under the heading that indicates findings, the first

5      paragraph obviously redacted on a number of points.

6      Then the unredacted last sentence, the committee has

7      seen no evidence that any votes were changed or that

8      any voting machines were manipulated.

9              You'd agree that the committee had access

10     to more information than you had access to in terms

11     of Russia's activities, right?

12 A.  I would.  Although, I would note that this is

13     carefully phrased, that they've seen no evidence.  So

14     it's, again, acknowledging the limits of the

15     capabilities of the intelligence community to acquire

16     such evidence, especially from systems that just

17     don't generate that kind of evidence.

18 Q.  And it's not your testimony that votes were changed

19     in any election, right?

20 A.  No, it's not.

21 Q.  And it's not your testimony that any voting machine

22     used in an election was manipulated, correct?

23 A.  No, it's not my testimony that any voting machine was

24     manipulated.  It's my testimony that the possibility

25     was there and that in significant cases if it had

Case 1:18-cv-05391-SCJ    Document 401-1    Filed 06/27/20    Page 47 of 243

J. Alex Halderman , Ph.D.                February 25, 2020

Fair Fight Action, Inc., Et Al. Vs. Raffensperger, Brad, Et Al.

Page 45

1        occurred, we might not know it.

2    Q.   If you could turn next to page 11.  Are you familiar

3         with Dr. Liles who testified to the committee?

4    A.   I'm sorry.  Where are you referring to?

5    Q.   Page 11.

6                    MR. HERMAN:  At the top.

7                    THE WITNESS:  Oh, I see.  I see.

8    BY MR. TYSON:

9    Q.   First bullet at the top.  Do you know who Dr. Liles

10        is?

11   A.   I don't recall who Dr. Liles is actually.

12   Q.   Okay.  Let me ask about the quote that's there.

13        Scanning for vulnerabilities, quoted in the report,

14        is analogous to someone walking down the street and

15        looking to see if you are home.  A small number of

16        systems were unsuccessfully exploited as though

17        someone had rattled the doorknob but wasn't able to

18        get in.  However, a small number of the networks were

19        successfully exploited.  They made it through the

20        door.

21                    Do you agree with that quote that's there

22        in terms of the activities that you're aware of in

23        the 2016 election?

24   A.   With regard to the voter registration system

25        activities, I do agree with that characterization.

Case 1:18-cv-05391-SCJ    Document 401-1    Filed 06/27/20    Page 48 of 243
J. Alex Halderman , Ph.D.                February 25, 2020
Fair Fight Action, Inc., Et Al. Vs. Raffensperger, Brad, Et Al.

Page 46

1   Q.   Do you agree with -- would you use this description

2        for any other systems beyond the voter registration

3        systems?

4   A.   I'm not sure I would use this description for other

5        systems beyond voter registration.

6   Q.   And why is that?

7   A.   Because the pattern of activities that involved

8        attempts to infiltrate vendor systems and then spread

9        to municipalities, those don't have this form of just

10       rattling the door.  Those were -- those were a

11       different shape of attack.

12  Q.   Okay.  Let's go next to the next page, page 12.

13       Right before the extensive series of redactions,

14       there's a statement that intelligence developed later

15       in 2018 bolstered Mr. Daniel's assessment that all 50

16       states were targeted.

17            Is that consistent with your understanding

18       of Russia's activities in the 2016 election?

19  A.   Yes, it is.

20  Q.   And as we've discussed, targeting is not necessarily

21       the same as manipulating or accessing.

22  A.   That's right.  It's probably step one.

23  Q.   Let's go now to towards the very end, page 59.

24  A.   Oh, 59.

25  Q.   Yeah.  Way towards the back.  So the page immediately

Page 47

1         prior, just for context, the recommendations of the

2         committee to secure the vote itself.  The first

3         bullet there recommends the purchase of more secure

4         voting machines and recommends that any machine going

5         forward should have a voter-verified paper trail and

6         remove or render inert any wireless networking

7         capability.  Do you agree with that recommendation?

8    A.   You're talking about the first bullet here?

9    Q.   Yes.

10   A.   On page 59.  I'm just making sure I'm looking at the

11        right -- I would go farther than that recommendation,

12        but I think that -- but I don't disagree with that as

13        it stands.

14   Q.   And as I understand your testimony so far, you would

15        say that this recommendation is not true of Georgia's

16        new voting system; is that correct?  Or is it true of

17        Georgia's new voting system?

18   A.   So I think this does apply to Georgia's new voting

19        system.  But as I said, I think just this

20        recommendation by itself is not enough to render the

21        voting system secure, and I would certainly go

22        farther.

23   Q.   So to make sure I have that right, you believe

24        Georgia's system complies with the recommendation of

25        this first bullet of the committee's recommendations,

Page 48

1            but you would go further than the committee, correct?

2    A.     Yes.  Based on the science that's happened since 2017

3           or since -- since the committee received its

4           testimony that's the basis of this.  Yes.

5    Q.     And the second bullet on that page indicates that

6           states should require that machines purchased from

7           this point forward are either EAC certified or comply

8           with the VVSG standards.  That's true of Georgia's

9           new system as well, correct?

10   A.     Yes.  I believe that is true of Georgia's system.

11   Q.     The third bullet recommends that --

12   A.     Although, actually, pardon me, I'm not sure about the

13          remainder of that bullet, whether Georgia's

14          contracting satisfies that.  So if you're talking

15          about the whole recommendation, my answer is I don't

16          know.

17   Q.     Got it.  So as to the first sentence, yes.  As to the

18          second sentence, you don't have enough information to

19          know.

20   A.     Not at this -- at this time.

21   Q.     The third bullet there indicates an effort to secure

22          the chain of custody for paper ballots, and there's a

23          recommendation related to time stamping when ballots

24          are scanned.  Do you see that recommendation?

25   A.     Yes.

Case 1:18-cv-05391-SCJ    Document 401-1    Filed 06/27/20    Page 51 of 243
J.  Alex Halderman , Ph.D.                    February 25, 2020
Fair Fight Action, Inc., Et Al. Vs. Raffensperger, Brad, Et Al.

Page 49

1    Q.    And do you know if Georgia's new system includes any

2          safeguards against the insertion of fraudulent paper

3          ballots?

4    A.    Any safeguards against the insertion of fraudulent

5          paper ballots?  I think there are some safeguards.

6    Q.    The fourth bullet recommends audits, as we've

7          discussed a little bit already.  And there's an

8          indication that as of August 2018, five states

9          conducted no post-election audit and fourteen do not

10         do a complete post-election audit.  Do you see that

11         statement?

12   A.    Yes, I do.

13   Q.    And in terms of the adoption of risk limiting audits

14         on a statewide level, do you know how many states

15         currently do a statewide risk-limiting audit?

16   A.    It's a small number.  It depends how you want to

17         define it exactly.  But perhaps two or three require

18         one at this point.

19   Q.    And when you say it depends on how you want to define

20         it, are there different definitions of risk limiting

21         audits?

22   A.    There are -- there are several complexities to RLA

23         legislation.  The question is also about when the

24         audit is required to be performed.

25   Q.    So some of the factors would be whether the audit is

Case 1:18-cv-05391-SCJ    Document 401-1    Filed 06/27/20    Page 52 of 243
J. Alex Halderman , Ph.D.                         February 25, 2020
Fair Fight Action, Inc., Et Al. Vs. Raffensperger, Brad, Et Al.

Page 50

1        pre-certification or post-certification, correct?

2   A.   Yes.

3   Q.   And some of the factors would be what level of risk

4        limit is set for the audit?

5   A.   Yes.

6   Q.   And so those variabilities affect how robust the

7        audit is.  Is that a fair way to characterize that?

8   A.   Those are among the factors that affect whether it's

9        likely to discover an attack, if one occurs.

10  Q.   And are you aware of Georgia's statutory requirements

11       related to risk limiting audits?

12  A.   Yes, I am.

13  Q.   And what do you -- I'm sorry.  You're aware that that

14       requires a pilot risk-limiting audit, correct?

15  A.   I'm aware that it does require a pilot by 2021, I

16       believe.

17  Q.   Are you aware whether Georgia has already conducted a

18       pilot risk-limiting audit of any kind?

19  A.   Yes.  On the county level.

20  Q.   And you're aware of the Georgia statutory requirement

21       that an audit be performed of the November 2020

22       election, correct?

23  A.   Yes.  Though, not a risk-limiting audit.  So there is

24       potential arbitrary risk that the audit could fail to

25       detect outcome changing fraud.

Page 51

1    Q.    But it is possible that Georgia may choose to conduct

2          a risk-limiting audit in November 2020, correct?

3    A.    I suppose it's possible that Georgia could make

4          whatever changes it wants to its election system

5          between now and November.

6    Q.    The reason I ask is -- and, again, I'm not asking for

7          your legal opinion on this.  But is it consistent

8          with your understanding that the requirement for

9          November 2020 is there must be an audit but not

10         requirements beyond that?

11   A.    That's consistent with my understanding.

12   Q.    If you could turn to page 61 of the recommendations.

13         The first bullet there indicates that states -- well,

14         I guess it's recommendations about grant funds.  But

15         it recommends improvements in cybersecurity like

16         hiring additional IT staff, updating software,

17         contracting with vendors to provide cybersecurity

18         services.  Is it your understanding those things are

19         happening in the State of Georgia related to

20         elections, or do you know?

21   A.    It's my understanding that those are happening to

22         some extent.  But you can tell from the way that this

23         is written that it's not simply a box to be checked.

24         These words mean -- these words imply a large range

25         of activities that if done with sufficient diligence

Page 52

1        will help, but it's more than simply having hired

2        someone.

3    Q.    All right.  So next I want to move to some of the

4        work that you've done in the public space.  I'm using

5        this next exhibit as a placeholder to talk about the

6        New York Times video.

7                  (Exhibit No. 9 marked.)

8    BY MR. TYSON:

9    Q.    So let me hand you what we've marked as No. 9.  And

10       this is a printout of New York Times story titled I

11       Hacked an Election.  So Can the Russians.  A video of

12       a part of a series on voting in America.  Do you

13       recall participating in this video series for the New

14       York Times?

15   A.    Yes, I do.

16   Q.    And can you describe generally what the videos in

17       this series involved?

18   A.    I actually haven't seen the other videos in the

19       series.  So I can only tell you about the video that

20       I participated in.

21   Q.    We'll start with yours then.  Why don't you tell us

22       about that video that you participated in?

23   A.    Right.  So that video was about risks to election

24       security that involve attacks on voting machines and

25       the potential for malicious software on voting

Page 53

1          machines to change the way votes are counted.

2     Q.   And were you approached by the New York Times, or did

3          you approach them to create this video?

4     A.   I was approached by them.

5     Q.   Okay.  And it's fair to say that the focus of the

6          video you participated in was to bring attention to

7          your area of research, correct?

8     A.   Was to bring attention to the risks to elections that

9          my research touches on.  Yes.

10    Q.   And ultimately bringing attention to that was part of

11         the goal to influence policymakers to abandon

12         electronic voting systems?

13    A.   Well, to influence general improvements to election

14         security.  That's right.

15    Q.   And one of those improvements to election security

16         would be abandoning electronic voting machines

17         without a paper trail, correct?

18    A.   Well, would be -- would be adopting machines that are

19         able to generate evidence where that evidence is

20         actually reviewed sufficiently in order for risks of

21         the equipment being hacked no longer to be a concern.

22    Q.   We talked earlier about the ethical implications of

23         certain types of hacking, hospitals and those kinds

24         of things.  Have you done any research or published

25         any research or given thought to the ethical

J. Alex Halderman , Ph.D.                          February 25, 2020
Fair Fight Action, Inc., Et Al. Vs. Raffensperger, Brad, Et Al.

Page 54

1            implications of saying elections could be hacked and

2            what that may mean for our system of government?

3     A.     Yes, I have given attention to that.

4     Q.     Have you published any papers on that topic?

5     A.     Yes, I have.

6     Q.     And could you point me to those in your CV?

7     A.     There's a paper entitled ethical implications of

8            electronic voting research or something like that,

9            which if you'll give me a copy of my CV, I can point

10           you to.

11    Q.     It's actually Exhibit 2.

12    A.     Thank you.  Oh, is that attachment to Exhibit 2 here.

13    Q.     Yes.

14    A.     Oh, where is that?  It would be reference 82 on page

15           57 of this document, page 13 of the CV.

16    Q.     And I'm assuming in that paper you've concluded that

17           it is ethical to discuss the security of election

18           systems, correct?

19    A.     It's a long discussion of various scenarios, but we

20           do touch on that topic, I believe.  It's been a long

21           time.

22    Q.     Now, in addition to your New York Times video, you've

23           also written an editorial in The Washington Post

24           about election security, correct?

25    A.     That's right.

J. Alex Halderman , Ph.D.                    February 25, 2020
Fair Fight Action, Inc., Et Al. Vs. Raffensperger, Brad, Et Al.

Page 55

1    Q.    I'm going to hand you what we've marked as Exhibit

2          10.

3                    (Exhibit No. 10 marked.)

4    BY MR. TYSON:

5    Q.    And I'll ask if that's your Washington Post

6          editorial.

7    A.    Yes.

8    Q.    And if you could turn with me to the fourth page

9          there.  The top of that page begins one simple answer

10         is that lawmakers need a straightforward policy

11         agenda to fix the system.

12                   So you were offering up a policy solution

13         that was recommended by your research; is that fair

14         to say?

15   A.    Well, so my research coupled with the political and

16         legislative dynamics.

17   Q.    And what political and legislative dynamics are you

18         referring to?

19   A.    Well, so this is recommending federal policy, and

20         there are certain questions about what's the

21         strongest level of security recommendation, for

22         instance, that would be likely to be passed by the

23         congress and signed by the president.  So it's

24         possible that the political compromises involved

25         there will result in a solution that's less than

Page 56

1         perfectly effective.

2    Q.   So you were advocating against or kind of in favor of

3         more secure voting systems and made these

4         recommendations based on what you thought was a

5         reasonable path forward politically; is that fair to

6         say?

7    A.   Or a plausible path forward politically in part.

8    Q.   Okay.  And so those recommendations include the

9         second paragraph there, replacing paperless voting

10        machines with systems that include a good old

11        fashioned paper ballot.

12   A.   Indeed.

13   Q.   And you personally believe that the best system would

14        replace paperless DRE machines and be a good old

15        fashioned paper ballot, correct?

16   A.   I do, in the sense of a ballot that is hand-marked by

17        those who are able to.

18   Q.   And you also wrote an article on the online platform

19        Medium about hacked elections in 2016.  Do you recall

20        that article?

21   A.   I do.

22              (Exhibit No. 11 marked.)

23   BY MR. TYSON:

24   Q.   So first of all, the reason for the article indicates

25        you wanted to set the record straight about

J. Alex Halderman , Ph.D.                    February 25, 2020
Fair Fight Action, Inc., Et Al. Vs. Raffensperger, Brad, Et Al.

Page 57

1           something.  Let me hand you what we've marked as

2           Exhibit 11.  I'll ask you first is that the article

3           that you wrote on Medium?

4    A.     Yes.

5    Q.     Okay.  So on the first page there, you indicate that

6           you wanted to set the record straight about what you

7           had been saying to the Clinton campaign and everyone

8           else who's willing to listen; is that right?

9    A.     That's right.

10   Q.     And so what record needed to be set straight?

11   A.     Right.  So there had been an article in New York

12          magazine that incorrectly attributed to me -- and

13          this is in the immediate aftermath of the 2016

14          election -- the view that I suppose that I thought

15          that the election had been -- result had been changed

16          my hacking.

17   Q.     Okay.  So on the second page then, underneath the

18          map, if you want to turn to that second page, there's

19          a statement in that paragraph right under the map,

20          were these year's deviations from pre-election polls

21          the result of a cyberattack?  Probably not.  I

22          believe the most likely explanation is that the polls

23          were systematically wrong, rather than that the

24          election was hacked.

25   A.     That's right.  At the time I think I would have said

J. Alex Halderman , Ph.D.                February 25, 2020
Fair Fight Action, Inc., Et Al. Vs. Raffensperger, Brad, Et Al.

Page 58

1        I think there's only, say, a 20 percent chance that

2        the result had been changed due to hacking of

3        election systems and an 80 percent chance that it was

4        due to the polling differences, but the implication

5        is a 20 percent chance is still pretty high and

6        someone probably ought to check.

7    Q.  And today do you still believe that kind of 80/20

8        possibilities of what resulted in the 2016 election

9        results?

10   A.  No.  I think that there was substantial more evidence

11       in favor of the election result being correct that

12       was gained because of the recounts that were

13       partially completed in Wisconsin and Michigan.

14   Q.  So if you could turn over to page 4.  The bottom of

15       that second paragraph before the headline in the next

16       section you say that many states continue to use

17       machines that are known to be insecure, sometimes

18       with software that is a decade or more out of date,

19       because they simply don't have the money to replace

20       those machines.  So would you take the position that

21       a state that did not replace its machines was

22       intentionally trying to make its elections

23       vulnerable?

24   A.  Well, it depends on -- it depends on the

25       circumstances.  And I think here and in other places

Page 59

1          where I am writing about states needing to replace

2          their machines, one thing that you'll see I keep

3          doing is mentioning that states need more funding,

4          and that is one of the policy goals that I've

5          consistently supported helping to make sure that

6          states like Georgia were getting additional funding.

7     Q.   So this was part of the effort -- the overall

8          advocacy effort to move away from more insecure

9          machines, get federal funding, help states see the

10         need.  Fair to say?

11    A.   I think my policy recommendations in those terms have

12         been consistent.

13    Q.   And then in the next -- the third paragraph under the

14         headline, you mention that we use two main kinds of

15         paper systems in the US.  And you reference first a

16         hand-marked paper ballot and second, a system that

17         prints a record on a piece of paper.  And so that

18         would refer to -- I'm sorry.  And then at the end of

19         the paragraph, you indicate that there's a record

20         that can't later be modified.  So at this time, were

21         you still advocating for ballot marking devices, or

22         was this still just only a subset for disabled

23         voters?

24    A.   I certainly wasn't advocating for ballot marking

25         devices.  But I think the keyword in that assessment

Page 60

1          is can't later be modified and the risk with many

2          ballot marking devices is that the record might be

3          modified before it gets printed and not noticed by

4          the voter.  And it's the same with VVPAT systems.

5                    (Recess taken.)

6     BY MR. TYSON:

7     Q.   All right.  Dr. Halderman, I'm going to hand you what

8          we've marked as Exhibit 12.

9                    (Exhibit No. 12 marked.)

10    BY MR. TYSON:

11    Q.   And this is a profile in apparently Michigan Alumnus

12         magazine.

13    A.   Oh, yes.

14    Q.   Have you seen this before?

15    A.   I have, yes.

16    Q.   So I'm assuming you were interviewed for this

17         publication.

18    A.   I was.

19    Q.   So if you could look with me at the first -- I'm

20         sorry, the second page titled Hacking the Vote, It's

21         Easier Than You Think.

22    A.   Yes.

23    Q.   Then the subhead line indicates that professor

24         J. Alex Halderman has made a career studying

25         electronic voting security.  His research has changed

Case 1:18-cv-05391-SCJ    Document 401-1    Filed 06/27/20    Page 63 of 243
J.  Alex Halderman , Ph.D.                February 25, 2020
Fair Fight Action, Inc., Et Al. Vs. Raffensperger, Brad, Et Al.

Page 61

1          the concept of stolen elections from theory to

2          reality.  Would you agree with that assessment that

3          elections have actually been stolen?

4    A.    Well, of course elections have been stolen.

5    Q.    Through hacking electronic voting machines?

6    A.    I think it's probably true that there have been

7          elections that have been altered as a result of a

8          cyberattack.  I can't point to one that successfully

9          was because if it was successfully altered, we

10         probably wouldn't know about it.

11   Q.    Okay.  Can you point to an unsuccessful example?

12   A.    Yes.

13   Q.    What is that?

14   A.    Well, one example is the 1994 election of Nelson

15         Mandela in South Africa where votes were tabulated by

16         electronic means.  And according to the UN and other

17         officials who were there at the time, somebody

18         successfully hacked into the computer network where

19         voters -- votes were being counted and attempted to

20         disadvantage Mandela's party, and that was detected.

21         But the interesting thing is the election officials

22         swore everyone to secrecy, and it wasn't until around

23         the time of Mandela's death that some of the

24         international officials involved started writing

25         about it in their memoirs.

Page 62

1              Another example would be the 2014 election

2         in Ukraine where attackers linked to Russia

3         reportedly attempted to -- reportedly did compromise

4         the election reporting system and rigged it to report

5         the wrong outcome, and that was apparently only

6         detected in the nick of time.

7    Q.   So let me rephrase my question then.  Are you saying

8         that any election in the United States has ever been

9         stolen through a hack of an electronic voting

10        machine?

11   A.   I can't point to a specific one.  But again, I think

12        there's substantial risk that one has that we don't

13        know about.

14   Q.   But sitting here today, you can't identify a single

15        election in the US that has had the result changed

16        through a hack of electronic voting systems?

17   A.   No.  Although, as I say, we probably wouldn't know.

18        That's one of the problems with electronic voting

19        systems.

20   Q.   If you could turn to page 9 of this profile.  And

21        that first full paragraph begins with -- let me just

22        read it.  The only reason there's no evidence of

23        whether voting machines or vote tabulating equipment

24        was hacked in the 2016 presidential election,

25        Halderman insists, is because nobody allowed him or

Page 63

1          anyone else to check.  And that's consistent with

2          what you've described earlier in terms of not being

3          able to do full recounts or analysis of electronic

4          voting machines after the 2016 election?

5    A.    Well, it's also referring to forensics on voting

6          systems and so forth.  Yes.

7    Q.    And so is it your testimony that there is evidence

8          that machines were hacked, and that if you looked,

9          you would find that, or you just don't know?

10   A.    If machines were hacked, there's a possibility that

11         evidence could be found by doing forensics of

12         individual machines.  That's my testimony.

13   Q.    Okay.  And the next sentence begins, this is the core

14         of his advocacy regarding electronic voting machines

15         and vote tabulators.  Would you agree with that

16         description of you as an advocate regarding

17         electronic voting machines and vote tabulators?

18   A.    I suppose it depends what you mean.  I certainly do

19         recommend specific policy measures that are necessary

20         to secure election systems.

21   Q.    The next page over, one, two, third full paragraph,

22         it talks about your preparation process for

23         testifying to the US senate committee with a murder

24         board.  Always a delightfully-named function.

25   A.    Indeed.  I'm not seeing where you mean.

Page 64

1    Q.    Right about in the middle of the page, third full

2          paragraph.

3    A.    It begins it was remarkable?

4    Q.    Yes.

5    A.    I see.  Yes.

6    Q.    And the last sentence of that paragraph says, the aim

7          was for Halderman to avoid seeming partisan.  Is

8          there a concern that election security issues are a

9          partisan issue at this point?

10   A.    They're certainly a non-partisan issue at this point,

11         as I think you can see by the broad bipartisan

12         support in congress for things like the Secure

13         Elections Act and the bill that Mark Meadows

14         introduced to adopt very similar protections.  But

15         there's always a risk in discussion of elections that

16         partisan politics will come into play.

17   Q.    But at this point, you are not aware of partisan

18         politics around the adoption of hand-marked paper

19         ballots?

20   A.    I was aware that -- I was aware, and I believe there

21         still is a risk that partisan politics will -- will

22         override the very real technical issues and make it

23         difficult to have strong security legislation.

24   Q.    Are you aware of the partisan breakdown of votes in

25         the Georgia General Assembly about hand-marked paper

Page 65

1          ballots versus ballot marking devices as an election

2          system?

3     A.   No, I'm not aware.

4     Q.   Would it surprise you if those were partisan votes?

5     A.   I think most votes are pretty partisan.

6     Q.   So it wouldn't surprise you?

7     A.   So it wouldn't surprise me.  Although, I'm not sure

8          which way the partisan politics would work out in

9          this particular issue in Georgia.

10    Q.   Going up that page just a little bit.  We talked

11         about your Medium essay, and this is a portion

12         discussing that.  You indicated that after you wrote

13         your Medium essay, you had come to a point of greater

14         confidence that the polling information was wrong

15         versus the election was hacked based on the partial

16         recounts that were conducted.  On that third

17         paragraph there, it indicates that the effort to

18         conduct recounts didn't succeed, and recounts were

19         only conducted in Wisconsin with minimal changes and

20         nobody was able to inspect any of the equipment.

21              What is it about the recount process that

22         changed your view from your Medium essay to now about

23         the 2016 election?

24    A.   That the recount involved in large parts of Wisconsin

25         and in parts of Michigan involved manual inspection

Case 1:18-cv-05391-SCJ     Document 401-1     Filed 06/27/20     Page 68 of 243

J. Alex Halderman , Ph.D.                    February 25, 2020

Fair Fight Action, Inc., Et Al. Vs. Raffensperger, Brad, Et Al.

Page 66

1           of ballots that had been marked by hand served to

2           provide additional evidence for the correctness of

3           the election results and that those manual

4           inspections of hand-marked records didn't reveal a

5           systematic deviation from the reported results.

6    Q.     There's also a reference in that paragraph that on

7           cable news and social media, you were dubbed a Stein

8           puppeteer trying to steal the election for Hillary

9           Clinton.  Is that an example of the partisan politics

10          that you discussed that could enter into those

11          questions?

12   A.     Yes.  I think that -- that experts being labeled

13          partisans merely because their views are inconvenient

14          for the views of a political group is a substantial

15          part of the risk.

16   Q.     There's also a great account in this article about

17          you meeting a man in a trench coat to obtain a

18          contraband voting machine.  Do you recall that event?

19   A.     I do.

20   Q.     And do you recall what kind of voting machine that

21          was?

22   A.     It was an AccuVote TS DRE.

23   Q.     That's the kind used in the State of Georgia up until

24          the end of 2019, right?

25   A.     That's correct.

Case 1:18-cv-05391-SCJ    Document 401-1    Filed 06/27/20    Page 69 of 243
J. Alex Halderman , Ph.D.                February 25, 2020
Fair Fight Action, Inc., Et Al. Vs. Raffensperger, Brad, Et Al.

Page 67

1    Q.    And on page 5 is where I am.  It's not necessarily

2          relevant.  It just mentions that you posted a video

3          about -- of the machine being hacked in a mock

4          election between Benedict Arnold and George

5          Washington.  Is that the same hacking demonstration

6          you performed for Judge Totenberg in 2018?

7    A.    I performed a similar demonstration.

8    Q.    But it wasn't the same type of hack demonstration?

9    A.    No.  Actually, it was using a different but also

10         effective way of hacking the AccuVote TS and TSX.

11   Q.    Okay.  And the demonstration that you did in the

12         YouTube video, would that have been untraceable to

13         someone looking at the voting machine?  Just in terms

14         of the main files, if they didn't dig into the system

15         architecture and just reviewed the reported files,

16         would that have been detectable in any way?

17   A.    No, it wouldn't have been detectable.

18   Q.    And just to stick with the 2016 recount piece for a

19         moment --

20   A.    You mean the Michigan Alumnus piece?

21   Q.    I'm sorry.  No.  Just the concept of doing recounts

22         following the 2016 election.  Not the exhibit.  We're

23         finished with the exhibit.

24               You assisted with the efforts to obtain

25         recounts in Michigan, Wisconsin, and Pennsylvania in

Case 1:18-cv-05391-SCJ   Document 401-1   Filed 06/27/20   Page 70 of 243

J. Alex Halderman , Ph.D.                    February 25, 2020

Fair Fight Action, Inc., Et Al. Vs. Raffensperger, Brad, Et Al.

Page 68

1        2016; is that right?

2   A.   Yes.

3   Q.   And were you retained by the Stein campaign or the

4        Clinton campaign?

5   A.   I was retained by the Stein campaign.

6   Q.   And did you assist with recounts in any other states

7        in 2016?

8   A.   No, just those three.

9   Q.   And all three of those states were won by President

10       Trump in 2016, correct?

11  A.   Yes.  That's correct.

12  Q.   And were these efforts you undertook pro bono, or

13       were you being paid by the campaign?

14  A.   I was being paid.

15  Q.   Have you ever worked as a staffer on any political

16       campaign?

17  A.   No, I haven't.

18  Q.   Have you ever been retained by political campaigns

19       beside the Stein campaign?

20  A.   No.  Oh, actually, strike that.  Yes, I have.  I have

21       on one other occasion.

22  Q.   And what campaign was that?

23  A.   That's the current political campaign for the

24       presidency of the Dominican Republic.

25  Q.   So I can clarify that quickly.  In the United States,

Page 69

1          you've not been retained by any other candidate or

2          campaign?

3     A.   No.

4     Q.   Okay.  Now, you hold at least one patent; is that

5          correct?

6     A.   Yes, that's correct.

7     Q.   I want to hand you what we've marked as Exhibit 13.

8                    (Exhibit No. 13 marked.)

9     BY MR. TYSON:

10    Q.   I'll ask if this is a patent that you hold as an

11         inventor.

12    A.   Yes, it is.

13    Q.   And what does this patent involve?

14    A.   This is a system for efficiently auditing elections

15         by using a high-speed scanner to review

16         electronically paper ballots and then using

17         statistical sampling similar to an RLA to confirm the

18         results.

19    Q.   Now, do you retain any financial interest in the use

20         of this patent going forward?

21    A.   No.  In fact, Princeton has dedicated it to the

22         public domain at my request.

23    Q.   If you could turn to the -- I guess it's the one,

24         two, three, fourth, fifth physical page.  The top

25         begins System and Method For Machine-Assisted

Case 1:18-cv-05391-SCJ    Document 401-1    Filed 06/27/20    Page 72 of 243

J. Alex Halderman , Ph.D.                February 25, 2020

Fair Fight Action, Inc., Et Al. Vs. Raffensperger, Brad, Et Al.

Page 70

1          Electronic Auditing.

2     A.   I'm sorry.  Can you repeat the page?

3     Q.   Sure.  The fifth physical page.

4     A.   The fifth -- the marked column 5 here?

5                    MR. HERMAN:  The actual.

6     BY MR. TYSON:

7     Q.   Yeah.  The actual fifth page.

8     A.   The pages I don't think are numbered.

9     Q.   Oh, I see.  The columns are numbered.  My apologies.

10         I'm not a patent lawyer.  If you could look at column

11         2, down where line 25 is.

12    A.   Yes.

13    Q.   There's an indication that the primary weakness of a

14         particular method you're referring to and discussing

15         is establishing a link between electronic and paper

16         ballots at the time votes are cast.  Is this issue of

17         voter privacy, that if we kind of sequentially number

18         every ballot as it's collected and could tie that

19         back to voters that are voting at particular times a

20         common issue you encounter in the design of audits

21         for election systems?

22    A.   Excuse me.  Let me just review those two paragraphs.

23    Q.   Certainly.  Yes.

24    A.   Yes.  Sequential numbering of ballots is a common

25         issue in audits and in the design of voting systems

Page 71

1        more generally and creates privacy risks.

2   Q.   The way I've thought about it is I've tried to think

3        about it in the past.  If we could maintain the link

4        between the person and the ballot, auditing would

5        probably be pretty simple I'm guessing at that point.

6        We could use some sort of log method for that.  But

7        the importance of the secret ballot that we have to

8        separate those two pieces of information, is it

9        correct to say that's what leads to a lot of the

10       challenges around how we handle ballots and how we do

11       audits?

12  A.   I would say that, more broadly than that, that the

13       need for a secret ballot complicates much of election

14       security.

15  Q.   Okay.

16  A.   If we could just print everyone's name and vote in

17       the newspaper, it would be much easier.

18  Q.   From a security standpoint, but not from a

19       constitutional or administrative standpoint, correct?

20  A.   In fact, it would be bad from a security standpoint

21       too because the secret ballot is an important defense

22       against certain attacks.

23  Q.   So printing everybody's votes in the newspaper would

24       help with some attacks but would lead to other

25       possible attacks.  Is that what you're saying?

Page 72

1    A.    That's right.

2    Q.    So in the election field, do you consistently find

3          these kinds of trade-offs, that doing one thing may

4          solve one problem but create a host of other

5          problems?

6    A.    That's right.  That's why we need to be -- that's why

7          only certain technological approaches achieve a high

8          level of security all around.

9    Q.    But you'd agree with me that if, for example, the

10         United States of America decided that the secret

11         ballot was no longer an important consideration as

12         just a policy matter, that would change the mix of

13         technology in what we used going forward, right?  I

14         know that's a wild hypothetical.

15   A.    That's a wild hypothetical.  If it was actually true,

16         contrary to reality, that the secret ballot wasn't

17         important, it would be easier to design secure

18         election systems.

19   Q.    Just out of curiosity, I'm sure you followed what's

20         happened with the Iowa caucuses.

21   A.    I have.

22   Q.    Is it possible there's some kind of hacking for that

23         system, or do you have -- have you done any research

24         or have any opinions about that system?

25   A.    On the Iowa caucus system?  What part of it do you

Case 1:18-cv-05391-SCJ    Document 401-1    Filed 06/27/20    Page 75 of 243
J.  Alex Halderman , Ph.D.                    February 25, 2020
Fair Fight Action, Inc., Et Al. Vs. Raffensperger, Brad, Et Al.

Page 73

1       mean?

2    Q.    I'm only going on news accounts that there have been

3          problems with the tabulation and an app that was

4          being used.

5    A.    Right.  Do you have a specific question?

6    Q.    It was just my own personal curiosity.  We can move

7          on.  Sorry.

8    A.    What a mess.  Let me just say what a mess.

9    Q.    All right.  So it's fair to say that you believe

10         electronic voting brings a host of problems to the

11         election system; is that fair to say?

12   A.    Yes.  It exposes the election system to several

13         different kinds of attacks.

14   Q.    Is there any circumstance besides disabled voters

15         where you would support the use of electronic

16         machines over hand-marked paper ballots?

17   A.    You mean ballot marking devices over hand-marked

18         paper ballots?

19   Q.    Any type of electronic ballot marker, whether done

20         through a DRE, through a ballot marking device, any

21         scenario.

22   A.    I see.  Is there any scenario?  In general, no.

23   Q.    So are you thinking of something besides disabled

24         voters where you might be willing to support

25         electronic voting?

J. Alex Halderman , Ph.D.                    February 25, 2020
Fair Fight Action, Inc., Et Al. Vs. Raffensperger, Brad, Et Al.

Page 74

1    A.    Well, I'm thinking, for instance, in some extreme

2          emergency, would it be -- would I be -- would I say I

3          would support it?  Well, it's hard to say.  It really

4          depends on the facts of the situation.

5    Q.    And it's fair to say that setting aside disabled

6          voters, you believe that hand-marked paper ballots

7          that are fully audited is the best method of

8          administering elections, right?

9    A.    I think from a security perspective, that's correct.

10   Q.    From an administerability standpoint, do you not

11         think that's correct, or is there a perspective where

12         you would disagree with that?  The reason why I

13         ask -- I can clarify.  I know you're trying to figure

14         out what I asked.

15               You clarified your answer with that you

16         believe from a security perspective that hand-marked

17         paper ballots with full audit to be the best method

18         of administering elections.  So my question is why

19         only from that perspective.

20   A.    Oh, I see what you mean.  There are -- there may be

21         administrative reasons to prefer other systems in

22         certain circumstances.  Although, I think the

23         alternatives do create a large and uncovered risk of

24         attacks to the election system.

25   Q.    So there may be policy reasons for using some

Case 1:18-cv-05391-SCJ   Document 401-1   Filed 06/27/20   Page 77 of 243
J. Alex Halderman , Ph.D.                        February 25, 2020
Fair Fight Action, Inc., Et Al. Vs. Raffensperger, Brad, Et Al.

Page 75

 1        electronic components, is that what you're saying,

 2        but it creates a security risk in the process?

 3   A.   Yes.

 4   Q.   I'm assuming that you don't believe that hand

 5        counting all ballots is the best possible system.

 6   A.   That's correct.

 7   Q.   And why is that?

 8   A.   Because hand counting all ballots -- hand counting

 9        all ballots would take a very long time.  Hand

10        counting we know also creates its own set of security

11        risks.

12              My perspective is that the best way to

13        administer and secure elections is to count ballots

14        electronically, but to confirm the results of the

15        electronic counting through manual follow-up.

16   Q.   So if we had a system that involved hand-marked

17        ballots that were hand counted, would you still think

18        audits were required in that scenario?

19   A.   Some kind of audit I would say would still be

20        required.  But it wouldn't be the same kind of audit

21        that would be an RLA, for instance, designed to

22        specifically detect errors in a machine count because

23        you wouldn't have a machine count.

24   Q.   And when you mentioned that hand counting can bring

25        other challenges, would that include election

Case 1:18-cv-05391-SCJ    Document 401-1    Filed 06/27/20    Page 78 of 243

J. Alex Halderman , Ph.D.                    February 25, 2020

Fair Fight Action, Inc., Et Al. Vs. Raffensperger, Brad, Et Al.

Page 76

1      officials overvoting a ballot, for example, during a

2      hand count?

3   A.   That's a potential risk.  If the election officials

4      are dishonest, they could potentially make changes to

5      the ballots during counting.  That's right.

6   Q.   And you think it would be best for the State of

7      Georgia to have a system of hand-marked paper ballots

8      as the primary means of voting, right?

9   A.   Yes, I do.

10  Q.   I'm going to change direction a little bit.  Are you

11     good to keep ongoing?

12  A.   Yeah.  Let's keep on going a little bit.  I assume

13     we're thinking of lunch at some point.

14  Q.   Eventually, yes.  Probably have a good stopping point

15     here in a little bit.

16              I want to talk about some general things

17     about your report, Exhibit 2.  If you want to get

18     that in front of you.  Talk about some high level

19     pieces to it first, and then move through some of the

20     specifics.

21              All right.  So through your report, is

22     there a particular section of your report that

23     summarizes the opinions that you offer in it?

24  A.   I'm not sure there's a particular section that does.

25  Q.   If you could go with me to paragraph 20.  When I was

Page 77

1          looking for it, it seems paragraphs 20 and 23 seems

2          to summarize things well.  If you want to get there,

3          it's on page 6 on the bottom, 7 on the top.

4     A.   Okay.

5     Q.   So in this -- in paragraph 20 to start with, you

6          identify your opinion about a variety of scenarios of

7          what could happen based on Georgia's election system

8          facing a high risk of being targeted.  Is that a fair

9          statement?

10    A.   Yes.

11    Q.   So you say, first sentence, that there's a high risk

12         of being targeted by sophisticated adversaries.

13         Second, those adversaries could attempt to hack the

14         election system.  Third, they could sabotage BMDs or

15         optical scanners.  Fourth, they could infiltrate BMDs

16         and optical scanners.  And fifth, those attacks could

17         succeed despite efforts that Georgia has put in

18         place.

19               Is that a fair list of things that you

20         think are the main problems from Georgia's

21         perspective?

22    A.   With the new system, I think it's fair to say that's

23         a good summary of much of what's in my opinion --

24    Q.   Okay.

25    A.   -- in my report.

Page 78

1    Q.    And you're not saying that these scenarios definitely

2          will happen or have happened.  You're just saying

3          they might happen, correct?

4    A.    I'm not saying they definitely will happen.  I'm

5          saying that there's a high risk that they might

6          happen.

7    Q.    You'd agree with me that every election system used

8          by every state is subject to the potential targeting

9          by sophisticated adversaries, right?

10   A.    Yes.  That's why in every election system in every

11         state things like hand-marked paper ballots and risk

12         limiting audits are an important defense.

13   Q.    And you'd agree with me that every election system

14         used by every state has the potential to be hacked,

15         right?

16   A.    Indeed.  Again, that's why these protections are so

17         essential.

18   Q.    And you'd agree with me that attackers could sabotage

19         components of the election system used in every

20         state, right?

21   A.    That's right.  Again, why these defenses are so

22         important.

23   Q.    And you'd agree with me that attackers could place

24         malicious software on BMDs or optical scanners in the

25         election system of every state, right?

J. Alex Halderman , Ph.D.                    February 25, 2020
Fair Fight Action, Inc., Et Al. Vs. Raffensperger, Brad, Et Al.

Page 79

1    A.    Where those components are used, that's right.  Very

2          few states use BMDs for all voters.

3    Q.    But all states use optical scanners, right?

4    A.    At least somewhere.  Not in all jurisdictions in all

5          states unfortunately.  There are still some paperless

6          jurisdictions.

7    Q.    And you'd agree with me that the kind of attacks that

8          we've outlined here could also succeed in other

9          states too, right?

10   A.    Yes.

11   Q.    So in approaching your opinion about Georgia's

12         election system, what kind of specialized knowledge

13         are you using to come up with these potential

14         scenarios if they could apply to every states'

15         election system?

16   A.    What do you mean by specialized knowledge?

17   Q.    Does it require any special training or experience to

18         be able to outline the scenarios you've outlined in

19         paragraph 20?

20   A.    Yes.  Yes, it does.

21   Q.    And what -- I'm sorry.  Finish.

22   A.    Yes, it does.  So I've been studying security risks

23         to electronic voting systems for getting close to 20

24         years now.  And so I think that kind of specialized

25         knowledge is important in assessing both the threat

J.  Alex Halderman , Ph.D.                    February 25, 2020
Fair Fight Action, Inc., Et Al. Vs. Raffensperger, Brad, Et Al.

Page 80

1          and the level of risk.

2     Q.   And so you do have specialized knowledge about kind

3          of the potential vectors of attack, I think as we

4          refer to them, on computers that are used in the

5          election system.  Fair to say?

6     A.   Yes.

7     Q.   And your focus has been primarily on the cyber

8          vulnerabilities of an election system, the computers

9          that are involved, not on the potential manipulation

10         of paper ballots through kind of old school methods.

11         We've referred to overvoting a ballot, for example.

12         Your research is focused primarily on the cyber

13         risks, right?

14    A.   I would say primarily.  But it also considers those

15         other risks, and I teach about them.  And auditing or

16         other defensive methods that I talk about are

17         designed with those risks in mind too.

18    Q.   So in reaching your opinions about Georgia's election

19         system, you are evaluating all the potential risks,

20         not only the cyber risks but also other possible

21         security risks?

22    A.   Well, I have thought about other potential security

23         risks, but the opinion here is primarily about the

24         risks of cyber attacks.

25    Q.   And in reaching your conclusion about Georgia's

Page 81

1          election system facing a high risk, is that including

2          the other security risks beyond cyber, or is that

3          limited to a cyber risk for the State of Georgia?

4     A.   Here I'm talking about the risks of attack by

5          sophisticated adversaries like hostile governments in

6          the context of attacks on computer system.

7     Q.   Okay.  And so in reaching your opinions in your

8          report, you've obviously used your specialized

9          knowledge to come up with a series of scenarios of

10         things that could happen.  And then you're assessing

11         how likely or unlikely those scenarios are to happen,

12         or are you just identifying these are possible

13         attacks?

14    A.   I'm also assessing the level of risk.

15    Q.   Okay.  And have you ever evaluated comparative risks

16         of an entirely paper ballot election system versus a

17         system that uses some electronic components?

18    A.   Of an entirely -- you mean a hypothetical?

19    Q.   Excepting disabled voters.  A hand-marked paper

20         ballot system for the comparative risk of that system

21         versus a system that uses electronic components.

22    A.   I have evaluated the risks in hand-marked paper

23         ballot systems, including for the Secretary of State

24         of Michigan.  So yes.

25    Q.   And what is the method you've used to evaluate the

J. Alex Halderman , Ph.D.                    February 25, 2020
Fair Fight Action, Inc., Et Al. Vs. Raffensperger, Brad, Et Al.

Page 82

1           comparative risks of those types of systems?  If

2           you're trying to compare one system's risks with

3           another, what is the method you'd used to evaluate

4           that comparative risk?

5     A.    So the method is basically what are -- examining the

6           differences between those voting systems and which

7           new attack vectors they make possible and how likely

8           are those vectors to be exploited.

9     Q.    So you essentially say okay, for system one, let's

10          say hand-marked paper ballot system with ballot

11          marking devices for disabled voters, electronically

12          tabulated using optical scanners, here's the list of

13          possible risks we face with that system?

14    A.    Of cybersecurity risks and which ones are enabled by

15          this change of technology.

16    Q.    And then we look at a system, ballot marking device

17          system for all voters, what are the risks with that

18          system.  So my question is, how do you then decide

19          which system is more or less secure based on that

20          list of risks?  Is there a specific method you use

21          for that?

22    A.    Sure.  So, for instance, in the ballot marking device

23          study that I published in January, we have a

24          quantitative method.  There was an equation in there

25          that will tell you based on the proportion of voters

J.  Alex Halderman , Ph.D.                    February 25, 2020
Fair Fight Action, Inc., Et Al. Vs. Raffensperger, Brad, Et Al.

Page 83

1         who are using a ballot marking device versus a

2         hand-marked system, what is the additional risk

3         that's created by -- that outcome changing fraud will

4         go undetected.

5    Q.   And that's specifically related to voters verifying

6         their paper ballots, right?

7    A.   Right.  Which is one of the very significant defenses

8         in an election system is voter verification.  That's

9         the premise of BMD security, that voters will

10        successfully verify.

11   Q.   And it's not your testimony that there exists one

12        perfectly secure voting system, right?

13   A.   There are voting systems that have greater or lesser

14        risk for certain important categories of attacks and

15        ones that have no risk of certain categories of

16        attacks.  So I think the -- which is more secure or

17        not is pretty clear.

18   Q.   You say which is more secure or not is pretty clear.

19        Would that be as to overall policy reasons for one

20        system or another, or which one is more or less

21        secure from a cybersecurity standpoint?

22   A.   Well, I'm speaking specifically from a cybersecurity

23        standpoint.

24   Q.   And as we covered earlier, there are scenarios where

25        policymakers may have interest beyond cybersecurity

Page 84

1        in selecting a particular election system, correct?

2    A.   There are other interests that come to play.  I

3        believe that there -- but I don't think that the

4        other interests, as they are practically manifested,

5        outweigh the cybersecurity advantages or

6        disadvantages that are part of that equation.

7    Q.   And you've gotten where I was trying to get to

8        earlier.  So then what is the way that you determine

9        whether the other policy reasons outweigh the

10       cybersecurity risks?

11   A.   Well, we could talk about that in the context of

12       specific policy questions that are coming to bear.

13       The question is to me the methodology that I would

14       apply is what are the alternative ways of achieving

15       this policy goal and are there practical

16       cybersecurity techniques that we could use to achieve

17       security under those circumstances.  And when the

18       outcome turns out to be no, we either have a system

19       that is at high risk of attack or not, I think that

20       the policy -- the policy balance outcome is pretty

21       clear.

22   Q.   And, again, the methods you're using to make that

23       policy balance outcome that you see is so clear is

24       you are looking at possibly alternative policies that

25       could have less cyber risk; is that a fair way to say

Page 85

 1      that?

 2  A.  Well, possible -- can you repeat the question?

 3  Q.  Sure.  I'm just trying to understand how you weigh

 4      the policy options of the other policy reasons why a

 5      jurisdiction may have for other systems versus the

 6      cyber basis.  And particularly I'm looking for what

 7      method are you using to conclude that hand-marked

 8      paper ballots are the right election system to be

 9      used.  You're reaching a conclusion they are.

10  A.  I see.

11  Q.  That's what I'm trying to understand.  What method

12      are you using for that evaluation?

13  A.  There's a very stark cybersecurity difference between

14      the hand-marked system and/or hypothetical or not

15      hypothetical BMD for all system.  And so given the

16      sort of starkness of that contrast, the question is

17      can you achieve those same -- the question to me is

18      can you achieve the same policy objectives well with

19      the hand-marked system.  Right?  And if you can

20      achieve those policy objectives well with the system

21      that is significantly more secure, then I believe on

22      the basis of that reasoning it's the -- it's the

23      superior choice.

24  Q.  And it's a policy interest of a state, is it not, to

25      have voter intent be clear?  Could that be a policy

Case 1:18-cv-05391-SCJ    Document 401-1    Filed 06/27/20    Page 88 of 243
J. Alex Halderman , Ph.D.                    February 25, 2020
Fair Fight Action, Inc., Et Al. Vs. Raffensperger, Brad, Et Al.

Page 86

1        interest for a state?

2    A.  That could be a policy interest.

3    Q.  And in that policy interest, you'd agree with me that

4        ballot marking devices are superior to hand-marked

5        paper ballots, right?

6    A.  Not necessarily.  So hand-marked paper ballots.  You

7        can also have the optical scanner reject ballots that

8        the scanner determines are not clearly marked, and

9        that's a feature of the Dominion system, in fact.

10   Q.  And in those scenarios, have you ever talked to

11       election officials about what voter behavior happens

12       when a scanner rejects an improperly marked hand

13       paper ballot?

14   A.  I have talked to election officials about that, yes.

15   Q.  What have they told you?

16   A.  Some election officials have told me, in fact, that

17       when -- some election officials have told me that

18       they worry about delay that's caused by that

19       scenario.  But other election officials have told me

20       that they already have their scanners programmed to

21       work in that way and it's fine.

22   Q.  And election officials may have concerns about voters

23       becoming frustrated in the process.  Have you heard

24       that from election officials?

25   A.  I've heard that about BMD-based elections as well as

Page 87

```
 1        hand-marked elections.  So that is a concern either

 2        way.

 3   Q.   And those would be other policy interests that might

 4        underlie the selection of one system over another

 5        unrelated to cybersecurity, correct?

 6   A.   There are other important considerations.

 7   Q.   So you'd agree with me that it's not possible to

 8        eliminate every attack vector against an election

 9        system, right?

10   A.   Not every attack vector.  I mean, someone could cut

11        the power to the entire state somehow and just render

12        absolute chaos.  But in terms of attack vectors that

13        involve -- that involve hacking the computer systems

14        that are used to administer the election or that are

15        in the polling place, it's possible to reduce the

16        risks to a minimal level.

17   Q.   And when you say reduce the risks to a minimum level,

18        how are you categorizing minimal risk versus other

19        types of risk?  What method are you using to arrive

20        at this is a minimal risk system?

21   A.   Well, let me be more clear than that.  It's possible

22        to eliminate the risk that hacking polling place

23        equipment is going to be able to change the election

24        outcome or cause significant disruption through a

25        well-designed system.
```

Page 88

```
 1   Q.   But it's not possible to eliminate all the risks.  I

 2        think we talked about earlier every election system

 3        is subject to being targeted by sophisticated

 4        adversaries.  Every election system could have some

 5        components of it hacked.  Every election system could

 6        have software put on optical scanners.  So I guess

 7        I'm trying to understand where you're concluding

 8        there's minimal risk if there's always going to be

 9        these vulnerabilities for any election system.

10   A.   Well, at the point where we can have a high and

11        quantifiable statistical probability of detecting and

12        correcting attacks of that form, I would say the risk

13        has been well constrained.

14   Q.   And ultimately, though, isn't that a policy decision

15        of what level of risk someone is willing to

16        encounter?

17   A.   Well, it's a policy decision -- is it a policy

18        decision?  Can you repeat the question?

19   Q.   So we're talking about all these different interests

20        that go into elections.  You can reduce it to a

21        statistically quantifiable number that we can have

22        confidence in a particular outcome.  But maybe in the

23        process, we're going to create long lines to do that.

24        There's all these competing policy interests in the

25        space of the design of an election system.  So what
```

Page 89

1       I'm trying to get to is at what point is it a policy

2       decision and at what point is it a scientific process

3       you're using to arrive at your conclusions in this

4       report.

5    A.    Well, I reject the notion that it's actually a

6       trade-off between long lines and good security.  But,

7       I mean, if there's a policy decision that we would

8       like the election system to be at high risk of attack

9       by foreign governments, I suppose that is a policy

10      decision too, but I don't think it's a policy

11      decision that I as someone who is an expert in

12      election cybersecurity would get behind.

13   Q.    Do you use online banking?

14   A.    I do.

15   Q.    And I'm sure -- I do too.  And there are risks, of

16      course, that online banking is subject to

17      manipulation, hacking, targeted by foreign powers,

18      right?

19   A.    Yes.  And, in fact, there are billions of dollars of

20      fraud every year reportedly in the financial sector

21      due to hacking.

22   Q.    But obviously you've chosen, I've chosen to use a

23      system that has some risk for the sake of

24      convenience; is that fair to say?

25   A.    Well, I think the risks in online banking are fairly

J.  Alex Halderman , Ph.D.                    February 25, 2020
Fair Fight Action, Inc., Et Al. Vs. Raffensperger, Brad, Et Al.

Page 90

1         well constrained for consumers because of things like

2         FDIC protection, and most fundamentally, because if

3         the money is gone, we're going few notice.  The same

4         can't be said unfortunately of election systems.  If

5         the result is wrong, it's not necessarily going to be

6         apparent to anyone.

7    Q.   And I believe I saw you have a cellphone.

8    A.   I do.  It's right here.

9    Q.   I do too.  And cellphones are subject to

10        manipulation, hacking, targeting by foreign powers,

11        right?

12   A.   Potentially.

13   Q.   And yet, we use those because we've chosen to

14        encounter a degree of risk for the sake of

15        convenience, right?

16   A.   Well, so, again, if my cellphone is hacked, we

17        won't -- that will not end up causing something like

18        a national election outcome to be wrong, I hope.  But

19        there are good reasons, including the vulnerability

20        of cellphones, that we don't, for instance, let you

21        vote using an app on your cellphone in elections in

22        Georgia.  That's because the risks are substantial.

23   Q.   So I guess thinking about those examples, is your

24        ultimate opinion in your report that Georgia

25        policymakers have chosen to take too great a risk by

Case 1:18-cv-05391-SCJ    Document 401-1    Filed 06/27/20    Page 93 of 243
J. Alex Halderman , Ph.D.                    February 25, 2020
Fair Fight Action, Inc., Et Al. Vs. Raffensperger, Brad, Et Al.

Page 91

1       using an all ballot marking device system election

2       system?

3   A.  So my opinion is that it's a very, very substantial

4       risk.  And if -- and yes, I would say that the

5       process in Georgia that has led to this risk has

6       resulted in an undesirable outcome from the

7       perspective of protecting the votes of the people of

8       Georgia.

9   Q.  So it's your opinion that Georgia policymakers have

10      chosen a path with too much risk to use for

11      elections, right?

12  A.  Yes, I think it's too risky a path.

13  Q.  And that opinion lines up with your personal views on

14      election administration, right?

15  A.  With my personal views?  How do you distinguish from

16      my professional views in this case?

17  Q.  I believe you said earlier that you believe the best

18      system for administering elections is a hand-marked

19      paper ballot system with ballot marking devices for

20      disabled voters.

21  A.  I see.  Yes, I think it's consistent with that.  It's

22      totally consistent with that, yes.

23  Q.  And so what scientific method are you using to

24      determine that Georgia policymakers have taken a path

25      with too great a risk?  There's obviously a point

Page 92

1          that you cross over a threshold.  What method do you

2          use scientifically to determine where that tipping

3          point is?

4     A.   Where that tipping point is?  Oh, I see.  Well, I

5          think the -- I think the tipping point -- that

6          question, it comes down to a -- it comes down to

7          applying the expertise that I have from evaluating

8          voting systems to ask the question, is this system

9          actually going to provide a strong defense or not.

10         And so there's -- it's a matter of -- it's a matter

11         of comparatively assessing those risks.

12    Q.   Are there published studies about evaluating

13         acceptable degrees of risk in the election context?

14    A.   Probably there are.  So if you look at, for instance,

15         the California top-to-bottom review studies that were

16         commissioned in 2007, those studies technically are

17         focused on vulnerabilities in specific pieces of

18         election equipment but come out with the policy

19         recommendation that they not be used because the risk

20         is unacceptable.

21    Q.   And that was a policy recommendation as the result of

22         that analysis, correct?

23    A.   That's right.

24    Q.   So you have the California top-to-bottom review.

25         Have you ever published papers on determining what

Page 93

1        the acceptable degree of risk in election systems is?

2    A.   Acceptable degree of risk.

3    Q.   And the reason why I ask is, again, you're saying

4        that Georgia policymakers have taken too much risk.

5        So how -- have you ever published a paper evaluating

6        the acceptable degree of risk?

7    A.   So the ballot marking device paper that I published

8        in January tries to assess some of that in part by

9        trying to quantify whether -- whether in a given

10        system attacks are going to be detected or not,

11        what's the probability that an attack would be

12        detected.  If the system is achieving an acceptable

13        degree of risk, that probability is going to be high

14        for plausible attacks.  If it's not, it's going to be

15        low.  You can indeed quantify some of these things.

16    Q.   Did you determine the exact percentage at which you

17        cross that threshold in your study of ballot marking

18        devices?

19    A.   No.  But it's quite often the case in science that

20        rather than a clean threshold, you just have a

21        breakdown between scenarios that result in a low

22        output value and a high output value.

23    Q.   And so beyond the BMD paper, you can't think of any

24        other papers you've published looking at the

25        acceptable degree of risk in an election system?

Page 94

```
 1   A.    I think that's the most quantitative one.

 2   Q.    But you can't think of any others?

 3   A.    Not off the top of my head.  But I have published a

 4         lot of papers in this area, so it's quite possible.

 5   Q.    Sure.  Is the field of determining an acceptable

 6         degree of risk in non-election context, are you aware

 7         of that being a discipline that people study what --

 8         when people encounter certain degrees of risk?

 9   A.    That's quite often a question that comes up in

10         matters of public policy and science.

11   Q.    But you didn't rely on any papers outside the

12         election context about assessing acceptable degrees

13         of risks in forming your opinions in this report,

14         right?

15   A.    No, I didn't.

16   Q.    A couple other global questions, and I think we'll

17         probably be at a good stopping point for lunch.

18         We'll dig into the details of the report after that.

19                 Kind of globally throughout the report

20         there's terms potentially, possibly, could happen.

21         There's a lot of scenarios of what might happen along

22         the way.  And I believe we covered this already.  But

23         you are not aware of anyone who's ever documented an

24         actual compromise of an election system using

25         electronic voting equipment in an actual US election,
```

J. Alex Halderman , Ph.D.                    February 25, 2020
Fair Fight Action, Inc., Et Al. Vs. Raffensperger, Brad, Et Al.

Page 95

1        correct?  And I know I added a bunch of qualifiers on

2        there.

3    A.  You mean a hostile compromise?

4    Q.  Any compromise --

5    A.  Any compromise?

6    Q.  -- in a US election system of an electronic voting

7        machine.

8    A.  Sure.  There are plenty of voting machines in US

9        elections used in US elections that have been

10       actually demonstratively compromised.

11   Q.  And what are some examples of those?

12   A.  The previous voting machines used in Georgia, the TS

13       and TSX that I personally compromised, those kinds of

14       machines.

15   Q.  My question was that were being used in an actual

16       election.

17   A.  Those machines were used in actual elections in

18       Georgia from 2002 until 2019.

19   Q.  What I'm trying to get to is not a machine generally,

20       a model type that is being used in an election, but

21       an actual machine in a precinct on election day in a

22       US election.

23   A.  I see.

24   Q.  Has anyone ever documented a case of one of those

25       machines ever being compromised?

Page 96

1    A.    I don't believe so.

2              MR. HERMAN:  Okay.  Off the record

3         for a second.

4                   (Recess taken.)

5              MR. TYSON:  Back on the record.

6    BY MR. TYSON:

7    Q.    All right.  Dr. Halderman, before lunch, I said we

8          were going to turn to your report.  I apologize.  I

9          do have one more thing I wanted to ask before we go

10         there.

11   A.    Yes.

12   Q.    You're on the board of advisors for the Verified

13         Voting Foundation; is that right?

14   A.    I am.

15   Q.    And can you briefly describe what the Verified Voting

16         Foundation is.

17   A.    The Verified Voting -- the Verified Voting Foundation

18         is a group that advocates for stronger election

19         security.

20   Q.    And when you say stronger election security, is it

21         primarily the cybersecurity component that you -- the

22         field that you work in?

23   A.    Yes.  Primarily.  It's a group that was founded

24         originally by computer scientists, and that's the

25         focus of their activity.

Page 97

```
 1   Q.   Got it.  Were you involved in developing the

 2        principles for new voting systems from the Verified

 3        Voting Foundation?

 4   A.   I don't think so.  No.

 5   Q.   Okay.  I'm going to hand you what I've marked as

 6        Exhibit 14.

 7                 (Exhibit No. 14 marked.)

 8   BY MR. TYSON:

 9   Q.   Have you seen this document before?

10   A.   Yes.  Well, actually, wait.  No.  There's a new set

11        of principles since -- since 2015, I believe.

12   Q.   Okay.

13   A.   Or a new set of positions that I have seen, but I

14        don't think I've seen this version.

15   Q.   And this is the one I got off the website.  So I

16        might have gotten the wrong one.

17                 I wanted to ask about a couple of these

18        principles.  So No. 1, the system should use human

19        readable marks on paper as the official record of

20        voter preferences and as the official medium to store

21        votes.  Does the Verified Voting Foundation, to your

22        knowledge, accept ballot marking device ballots as a

23        valid way of voting, or is it only hand-marked

24        ballots?

25   A.   I believe that their current set of -- their current
```

Page 98

1          set of positions on these issues point to elevated

2          risk with ballot marking devices.

3     Q.   Let me ask about No. 7.  One of the other principles

4          is to use commercial off-the-shelf hardware and

5          open-source software.  Do you agree with that

6          principle of security in voting systems?

7     A.   Yes, I think all else being equal, that's probably

8          something that is at least somewhat preferred,

9          although commercial off-the-shelf hardware and

10         open-source software can also still have significant

11         security risks.

12    Q.   Okay.  Is there a reason just from a cybersecurity

13         perspective to prefer commercial off-the-shelf

14         hardware versus custom-built hardware?

15    A.   There is a reason to prefer it.  Again, all else

16         being equal, in general, developing hardware is

17         difficult and off-the-shelf hardware is more likely

18         to have been well tested than hardware that is

19         proprietary.  But it really depends on the specific

20         case whether it actually achieves security benefits

21         or not.

22    Q.   And does the same set of principles apply to

23         open-source software versus I'm assuming

24         custom-designed software?

25    A.   Yes.  Although, open-source software has the

Case 1:18-cv-05391-SCJ    Document 401-1    Filed 06/27/20    Page 101 of 243
J.  Alex Halderman , Ph.D.                February 25, 2020
Fair Fight Action, Inc., Et Al. Vs. Raffensperger, Brad, Et Al.

Page 99

1       additional benefit of making the code available to

2       others to review, which carries with it additional

3       security benefits since it's open to broader scrutiny

4       for problems.

5    Q.  And so since it's open to broader scrutiny, people

6       could find vulnerabilities and notify whoever they

7       need to to repair them; is that the general

8       principle?

9    A.  Well, that's right.  And so it's -- in addition, it

10      makes it easier to I think credibly assess the likely

11      level of security of the piece of software.  When

12      it's closed, it can be more challenging.

13   Q.  What is the role of kind of trade secret in voting

14      software particularly versus an open-source approach?

15      Are there pros and cons security-wise to each, or is

16      one always preferred over the other?

17   A.  I would say there are pros and cons.

18   Q.  And can you give me some examples of what the pros of

19      trade secret and what the pros of open source would

20      be?

21   A.  Well, the broader principle is that in a system that

22      is important for security, the parts that need to

23      remain secret for security should be well defined.

24      This is called Kerckhoffs' principle.  It's sort of a

25      foundation principle in security.  And it's easier to

J.  Alex Halderman , Ph.D.                    February 25, 2020
Fair Fight Action, Inc., Et Al. Vs. Raffensperger, Brad, Et Al.

Page 100

1           achieve that in an open-source system than a

2           closed-source sytem because in the closed-source

3           sytem, everything is being kept secret.  You might

4           not be able to compartmentalize the pieces that need

5           to be kept secret.  But yes, there's a need to keep

6           some secrets secret in basically any secure system.

7           But they should be limited to things like

8           cryptographic keys that are well defined and narrow.

9           That's the principle.

10    Q.    All right.  Well, let's go ahead and turn to your

11          report.  And the good news, we can skip ahead to

12          paragraph 14.  So we'll start on page 3.  What I

13          wanted to do primarily, just kind of walk through the

14          report and ask about some of the conclusions you've

15          reached and some of the decisions or the opinions

16          that you've offered in this case.

17                    So first of all, you indicate in paragraph

18          14 that you were asked to opine on the security of

19          Georgia's election system following the

20          implementation of the new system.  Is it your

21          understanding that the Dominion voting system and the

22          KnowInk system is at issue in this case?

23    A.    Yes, it's my understanding that it's at issue in this

24          case.

25    Q.    And you walk through the various components of that,

J. Alex Halderman , Ph.D.                    February 25, 2020
Fair Fight Action, Inc., Et Al. Vs. Raffensperger, Brad, Et Al.

Page 101

1           the ballot marking devices, the ICX component, the

2           ICP precinct scanners, the ICC central-count

3           scanners.  Have you personally observed and tested an

4           ICX ballot marking device?

5     A.    No, I have not.

6     Q.    Have you personally observed and tested an ICP

7           precinct-count scanner?

8     A.    No, I have not.

9     Q.    Have you personally observed and tested an ICC

10          central-count scanner?

11    A.    No, I have not.

12    Q.    Have you personally observed and tested the Democracy

13          Suite election management system?

14    A.    No, I have not.

15    Q.    And have you personally examined and tested any Poll

16          Pad electronic poll books?

17    A.    No, I haven't.  My views on the systems are based on

18          the experience that I've had over the last nearly 20

19          years with other electronic voting systems and the

20          design of the systems as documented by Dominion and

21          the tests that have been conducted in other states.

22    Q.    Okay.  So it's not based on any personal evaluation.

23          It's based on your knowledge, tests of others, and

24          understanding of the system from Dominion itself?

25    A.    That's right.

J. Alex Halderman , Ph.D.                    February 25, 2020
Fair Fight Action, Inc., Et Al. Vs. Raffensperger, Brad, Et Al.

Page 102

1    Q.    Okay.  And I believe in 15 we've already covered that

2          you reviewed the documents the plaintiffs provided to

3          you from Dominion.  Let's go to paragraph 16 about

4          the eNet software.

5    A.    Yes.

6    Q.    And eNet is Georgia's voter registration database,

7          correct?

8    A.    That's correct.  It's the software that runs the

9          voter registration database and some associated

10         administrative functions.

11   Q.    Do you know approximately how many states use eNet?

12         Is it a widely-used piece of software?

13   A.    There are versions of eNet used in other states.  I

14         know that.

15   Q.    Are there other voter registration database software

16         that is more widely used than eNet, or is eNet kind

17         of one of the main players in this space?

18   A.    It certainly is a player in this space.  But there

19         are different versions of the software that are used

20         in other states, some of which are relatively better

21         protected.

22   Q.    Okay.  And have you evaluated the protection of

23         Georgia's version of eNet versus the versions in

24         other states?

25   A.    So I am familiar with the -- I have personally

J.  Alex Halderman , Ph.D.                    February 25, 2020
Fair Fight Action, Inc., Et Al. Vs. Raffensperger, Brad, Et Al.

Page 103

1         evaluated vulnerabilities in the MVP and OVR system

2         compared to other states as a component of the

3         broader eNet platform.

4    Q.   Is it your testimony that MVP and OVR are part of the

5         eNet system?

6    A.   Are interfaced with it.  That's right.

7    Q.   And when you say interfaced with it, what do you mean

8         interfaced with it?

9    A.   I mean that data from those systems feeds into the

10        overall voter registration system and vice versa.

11   Q.   And does that happen without human intervention, or

12        is there a human intervention component for either of

13        those MVP and OVR systems to alter the voter

14        registration database?

15   A.   There may be a human component for the -- some of the

16        data that's fed back in.  I think the data that comes

17        out is read out by a computer process.

18   Q.   You say in paragraph 16 -- actually, before we go to

19        that, you said you evaluated the MVP and OVR

20        components.  Have you evaluated the eNet version used

21        by Georgia versus the eNet versions used by other

22        states?  For eNet specifically, not for other

23        associated applications.

24   A.   No, I have not.

25   Q.   You say in the second sentence of paragraph 16 that

Page 104

1          election officials use eNet to manage voter

2          registration data.  Which election officials use eNet

3          to manage voter registration data in Georgia?

4     A.   I'm not sure in Georgia's practice.

5     Q.   And do you know which election officials export eNet

6          data to electronic poll books?

7     A.   I don't know.  I think that happens at the Secretary

8          of State's office.  That's my understanding, but I --

9          but I'm willing to be corrected.

10    Q.   In the next sentence you talk about interface of MVP

11         and OVR and say that those systems allow voters to

12         view and update their voter registration data.  Can

13         you explain to me how those systems update voters'

14         voter registration data in eNet?

15    A.   So the voter can fill in updated information through

16         the voter -- or an updated -- or fill out a voter

17         registration -- a voter registration form on those

18         systems.  It gets uploaded to the server.  And then

19         through back-end processes, which may or may not

20         require human intervention, I'm not sure, the data is

21         updated in the voter registration database.

22    Q.   So you don't know if a voter registrar is required to

23         review information and changes to voter registration

24         data before those changes are made in eNet?

25    A.   You know, I'm not sure that it makes a significant

Page 105

1           difference to the security of the system overall.

2           Even attacks that could affect -- attacks could

3           affect voter registration in plausible ways that a

4           registrar would approve.

5     Q.    So it's your testimony that there's really no

6           security difference whether the input of a registrar

7           is required before changes are made?

8     A.    It matters to some kinds of attacks, but I don't

9           think to plausible attacks that could affect -- to

10          certain plausible attacks that could affect the --

11          could affect the ability of Georgia voters to cast

12          their votes on an election day.

13    Q.    And then we'll come back around to that in a little

14          bit more later on.  In paragraph 17, the bottom of

15          that page 4 you indicate absentee voters will not use

16          BMDs.  That is for people who vote absentee by mail;

17          is that right?

18    A.    That's my understanding.

19    Q.    And voters who vote absentee in person, do you have

20          an understanding of whether they will use BMDs or

21          not?

22    A.    I think absentee in person is a BMD process.  Yes.

23    Q.    In paragraph 18, you indicate in the second sentence

24          that the Secretary of State will transmit the

25          election programming files to county officials.  Do

Page 106

1        you know how that transmission is made?

2   A.   I'm not sure whether the process has been changed

3        from the process that was used prior to the

4        introduction of the Dominion system or not.  But the

5        process prior to the transmission via CD ROM has

6        significant security downsides.

7   Q.   Okay.  But you don't know the current setup that's

8        being used, correct?

9   A.   I'm not sure that it makes a difference for the kinds

10       of attacks that I'm worried about.  But I don't know

11       for sure the current process.  I'm not sure that

12       that's been documented publicly yet.

13  Q.   So it's your testimony that the method of

14       transmission doesn't really matter to the types of

15       attacks you're concerned about?

16  A.   To some of the attacks I'm concerned about.  That's

17       correct.

18  Q.   But it does matter to other types of attacks you're

19       concerned about?

20  A.   That's right.  There can be attacks that depend on

21       the specific method of transmission, and there are

22       other attacks that only depend on the fact of

23       transmission.

24  Q.   So in evaluating the relative risks to Georgia's

25       election system, you didn't consider the method of

Page 107

1          transmission as informing that part of risk

2          assessment, correct?

3    A.    I think the method of transmission -- excuse me.

4               (Discussion off the record.)

5    BY MR. TYSON:

6    Q.    So in reaching your conclusions about the risks faced

7          by Georgia's election system, you did not -- since

8          you did not know the method of transmission, you

9          didn't take the method of transmission into account

10         in making that assessment; is that right?

11   A.    Well, I think that's right.  The method of

12         transmission might change the level of risk around

13         the edges, but it's not likely to be a night and day

14         difference.

15   Q.    So it's not important to your overall conclusions; is

16         that right?

17   A.    No, I don't think it affects the overall conclusion.

18   Q.    Okay.  At the bottom of 18 you indicate that election

19         workers will install a memory card or USB stick into

20         each BMD and ICP scanner prior to the start of

21         voting.  Do you know which election officials or

22         workers will do that?

23   A.    My understanding is that in Georgia that usually

24         happens at the county, but I'm not completely sure.

25   Q.    Okay.  And then the removal in paragraph 19 of the

Page 108

1        memory cards for return, do you know which election

2        workers those would be?

3    A.   I think that happens at the polling place in Georgia,

4        but I'm not entirely sure.

5    Q.   And you don't mention what happens to the paper

6        ballots after an election.  Is that -- I'm assuming

7        that's not relevant to your analysis either.

8    A.   Well, not primarily to the cyber -- well, actually,

9        that is something that is relevant to the analysis.

10       I just don't mention it here.

11   Q.   So what is the method that the paper ballots are

12       returned back to a county official?

13   A.   I don't know.  But I'm assuming for purposes of this

14       analysis that the paper ballots are going to be

15       returned through an adequate chain of custody because

16       otherwise the security situation is even worse.

17   Q.   Okay.  So then you're assuming that paper ballots are

18       returned through an adequate chain of custody as part

19       of reaching your conclusions about the relative risks

20       of Georgia's system, right?

21   A.   Well, that's right, because those risks are even

22       worse if the chain of custody is not adequate.

23   Q.   And since you don't know exactly who's installing

24       memory cards, who's removing memory cards, I'm

25       assuming that's not part of your analysis either as

Case 1:18-cv-05391-SCJ    Document 401-1    Filed 06/27/20    Page 111 of 243

J.  Alex Halderman , Ph.D.                February 25, 2020

Fair Fight Action, Inc., Et Al. Vs. Raffensperger, Brad, Et Al.

Page 109

1        far as reaching your conclusions about relative risk.

2   A.   I tried to make generous assumptions about those

3        risks where I don't know the answer, ones that the

4        level of risk doesn't depend on it being the worst

5        possible way it could be done.

6   Q.   Again, so likely paper ballot transmission, you

7        assumed then that qualified election workers are

8        going to handle memory cards at all stages with the

9        proper chain of custody; is that fair to say?

10  A.   That's right.  Even though there are still

11       limitations to effectively what you can achieve with

12       that kind of chain of custody.

13  Q.   And --

14  A.   And also, I do -- okay.  That's fine.

15  Q.   We've already covered paragraph 20 I think pretty

16       thoroughly.  I just wanted to ask, on this point, the

17       high risk of attack that you're concerned about for

18       Georgia elections, would you say that Georgia's new

19       election system faces the same level of risk as the

20       DREs, a greater level of risk, or less risk?

21  A.   I think for very important -- for probably the most

22       important category of risk, which is the risk of

23       nation state attacks against close elections, the

24       risk is not substantially reduced.  I think for other

25       scenarios, there are some benefits to security from

Page 110

1       the change.  But sort of the thing that we all should

2       be most worried about, the security of the new system

3       is not -- is not such that those attacks are strongly

4       prevented.

5   Q.  So it's your testimony that Georgia faces basically

6       the same amount of risk from a nation state attacker

7       with its new voting system as it faced with the DRE

8       system; is that right?

9   A.  Unfortunately largely because of the lack of strong

10      auditing and the difficulty of verifying -- of voters

11      actually verifying their ballots well.

12  Q.  If Georgia implemented proper, as you would

13      categorize them, robust auditing procedures, would

14      the security situation from a nation state attacker

15      be improved over the DREs?

16  A.  Well, the problems are both the lack of robust

17      auditing and the lack of -- and the lack of a

18      strongly voter-verified paper record.  If both of

19      those things were corrected, then I think the

20      relative risk would be lower than in the DRE system.

21  Q.  And you used a distinction there that I want to hone

22      in on for a minute.  You refer to a voter-verified

23      paper record.  Can you describe the difference in a

24      voter-verifiable paper record and a voter-verified

25      paper record?

J. Alex Halderman , Ph.D.                    February 25, 2020
Fair Fight Action, Inc., Et Al. Vs. Raffensperger, Brad, Et Al.

Page 111

1    A.    Sure.  So with the caveat that those terms are often

2          not used precisely in the literature and people for

3          years kind of use them interchangeably but without

4          really addressing the question of whether things that

5          were verifiable would be verified.  But a

6          voter-verifiable record is one that in principle the

7          voter could verify.  A voter-verified record is one

8          the voter actually has verified and ensured is

9          correct.

10   Q.    And so in recommendations, there has been a lot of

11         terminology thrown around of voter-verifiable paper

12         records.  Voters have the option of verifying their

13         records in that situation, which distinguishes it

14         from a DRE where there would be no record; is that

15         correct?

16   A.    From a paperless DRE where there would be no record.

17   Q.    Yes.  I'm sorry.  Good clarification.  When I think

18         of DRE, I've only ever voted on a paperless DRE in

19         Georgia.  So thank you for that.

20              In paragraph 21, you say that there is no

21         doubt that Russia and other adversaries will strike

22         again.  On what basis are you saying that there is

23         absolutely no doubt they will strike again?  I'm

24         assuming you've not talked to President Putin or Vigo

25         Carpathian or somebody about this, right?

J.  Alex Halderman , Ph.D.                    February 25, 2020
Fair Fight Action, Inc., Et Al. Vs. Raffensperger, Brad, Et Al.

Page 112

1    A.    No.   But I follow very closely the assessments of the

2          intelligence community and DHS and the federal

3          government on these questions.  And there's every

4          indication that Russia continues at this very minute

5          to be attempting to interfere in the election.

6    Q.    And election interference we can draw as a distinct

7          concept from vote manipulation.  Wouldn't you agree

8          those are distinct concepts?  Maybe one includes the

9          other?

10   A.    Yeah, maybe one includes the other.

11   Q.    So election interference could include manipulating

12         votes.  But merely interfering could be spreading

13         false messages on social media, visiting websites of

14         county boards, scanning for vulnerabilities in a

15         system.  Would that be a fair distinction to draw?

16   A.    I think that's fair.

17   Q.    And so in terms of, you know, no doubt that Russia

18         will strike again, I think we covered earlier we

19         don't have any evidence that Russia manipulated votes

20         in any election in the US, correct?

21   A.    That's right.  Even though there were significant

22         gaps in the visibility that would make that evidence

23         available.

24   Q.    Over on the next page, page 7, you indicate that the

25         report found that these foreign agents were

J. Alex Halderman , Ph.D.                              February 25, 2020
Fair Fight Action, Inc., Et Al. Vs. Raffensperger, Brad, Et Al.

Page 113

1       successful in attacking at least one state.  Was that

2       one state Georgia?

3   A.  No.  Not the state that is referred to in the report.

4   Q.  In the last paragraph you indicate that Georgia was

5       among the states Russia targeted.  And as we

6       discussed earlier, targeting doesn't necessarily mean

7       manipulation or compromise, right?

8   A.  No.  It's just the first step, but it does -- it does

9       speak to -- towards the intent.

10  Q.  And like the Senate Intelligence Committee, the

11      special counsel never found any votes were actually

12      compromised, right?

13  A.  That's right.  But again, there were very serious

14      limitations to the available evidence that would, if

15      the votes were compromised, allow us to reach that

16      conclusion.  So the best I think that they could say

17      is well, essentially there's no evidence votes have

18      been compromised.

19  Q.  Is it your personal belief that Russia has

20      compromised votes in elections in the US?

21  A.  I don't know.

22  Q.  In paragraph 22, you talk about some examples.  I

23      believe we discussed earlier the Ukrainian

24      presidential election.  And Ukrain's vote counting

25      infrastructure that you reference there, that was a

J. Alex Halderman , Ph.D.                    February 25, 2020
Fair Fight Action, Inc., Et Al. Vs. Raffensperger, Brad, Et Al.

Page 114

1          system directly connected to the internet; isn't that

2          right?

3     A.   Yes, it was.

4     Q.   At the end of paragraph 22 you say, other adversarial

5          governments and various things might target future

6          Georgia elections.  And sitting here, you don't have

7          any evidence that other adversarial governments

8          absolutely will target Georgia elections, do you?

9     A.   No.  But there's no reason to doubt that other

10         governments have something at stake in the outcome of

11         future US elections and have the cybersecurity

12         offensive capabilities that they would need in order

13         to -- in order to do that.

14    Q.   But as we talked about, there's a difference in

15         aiming a gun and pulling the trigger, correct?

16    A.   That's correct.

17    Q.   And so you don't have any evidence they will

18         definitely pull the trigger to attack Georgia

19         elections?

20    A.   No, I can't speak to that.

21    Q.   To paragraph 23.  This is another kind of summary

22         opinion piece.  It's your opinion that Georgia's new

23         voting technology does not achieve the level of

24         security necessary to withstand an attack by a

25         sophisticated adversary, such as a hostile foreign

Page 115

```
 1        government.  Isn't that statement true of every

 2        states' voting technology?

 3   A.   So no, I don't think that it is true of every -- of

 4        every states' voting technology, at least not in the

 5        same sense, because in states that really do have a

 6        hand-marked ballot and are or are intending to audit

 7        the paper trail rigorously, the attacks that I'm most

 8        concerned about, ones that would actually change the

 9        election outcome, would not be likely to succeed.

10   Q.   So in your opinion, the necessary preconditions to

11        have the level of security necessary to withstand an

12        attack by a foreign government are hand-marked paper

13        ballots and robust audits; is that fair to say?

14   A.   Those are two of the most important, and there are

15        other components of resiliency that are important

16        too.

17   Q.   So do you have an estimate on what percentage of

18        jurisdictions currently have sufficiently robust

19        audits and hand-marked paper ballots to withstand

20        that kind of attack?

21   A.   It's just a few percent of jurisdictions

22        unfortunately.  There's still a lot of work to do

23        nationally.  But there are degrees.

24   Q.   So would it be fair to say then that 90 percent of

25        jurisdictions don't have the level of security
```

Page 116

1        necessary to withstand an attack by a hostile foreign

2        government?

3    A.  I'm not sure about 90 percent, but it is a high

4        percentage.

5    Q.  Higher than 80?

6    A.  Probably.

7    Q.  Okay.  Now, you have a lab where you do work related

8        to election technology and cyber vulnerabilities,

9        right?

10   A.  I do.

11   Q.  And do you believe your lab has the level of security

12       necessary to withstand an attack by a sophisticated

13       adversary such as a hostile foreign government?

14   A.  No, absolutely not.  We are -- we are definitely not,

15       however, running an election system for any state out

16       of our lab.

17   Q.  You do have technology in your lab that could be used

18       to compromise voting systems that are currently in

19       use, though, right?

20   A.  Yes, we do.  We try to take the best steps that we

21       can to prevent that.  But unfortunately, the reality

22       is that sophisticated nation states have -- hostile

23       nation states have extremely sophisticated cyber

24       offensive capabilities.  And the question is more a

25       question of do they really want to attack us, than

Page 117

1          can we withstand the determined attack.

2     Q.   So then in the subparagraphs under 23, you provide

3          some scenarios under which attackers could

4          potentially subvert the election technology.  And the

5          first is infiltration of the voter registration

6          database to extract, change, or erase records.  Do

7          you see that?

8     A.   Yes.

9     Q.   Do you have any evidence that that has ever happened

10         to the State of Georgia's voter registration

11         database?

12    A.   No, I don't.

13    Q.   And it's true that attackers could infiltrate the

14         voter registration database of any state if they were

15         a sophisticated hostile foreign government, right?

16    A.   That's probably true.  Although, Georgia's system has

17         specific technical risks that lead me to believe that

18         the risk is higher in the State of Georgia than in

19         other states.

20    Q.   And how many other states' voter registration

21         databases have you studied for potential risks?

22    A.   How many?  That's a good question.  A handful of

23         other states.  Certainly Michigan in great detail.

24    Q.   And when you say a handful, less than five?

25    A.   Probably less than five in detail.

Page 118

1    Q.    So you've evaluated five states or less of the voter

2          registration databases.  And of those, your

3          conclusion is that Georgia is the most vulnerable of

4          those five?

5    A.    I'm not sure that I've specifically ranked or

6          quantified, but I would say Georgia is significantly

7          more vulnerable than it needs to be.

8    Q.    As compared to those five other states?

9    A.    And as compared to some other states that I've

10         studied.  It's certainly more vulnerable that

11         Michigan's.

12   Q.    And what other states have you studied?

13   A.    Where else have I studied?  I've looked at the voter

14         registration technology in Pennsylvania and in

15         California to some degree.  I would have to go back

16         and check.

17   Q.    Okay.  And your analysis of the relative risk level

18         is based on -- what kind of factors are you reviewing

19         when you're evaluating the risk to the voter

20         registration databases?

21   A.    Some of the most important factors are things like

22         the age and brittleness of the software involved, who

23         is maintaining it, and what the results of security

24         assessments have been and whether the problems found

25         in those assessments have been completely mitigated.

J.  Alex Halderman , Ph.D.                    February 25, 2020
Fair Fight Action, Inc., Et Al. Vs. Raffensperger, Brad, Et Al.

Page 119

1    Q.    And have Michigan, Pennsylvania, California conducted

2          sophisticated threat assessments by cybersecurity

3          vendors of their voter registration databases?

4    A.    Michigan has.  I don't know about the other states.

5    Q.    And did those -- for Michigan, did they find any

6          potential vulnerabilities in the database?

7    A.    They did.

8    Q.    And did Michigan then mitigate those and correct

9          those?

10   A.    They did.

11   Q.    And did they correct all of them?

12   A.    To my knowledge, they did, yes.  In fact, they

13         replaced the entire software system as a result of

14         those analyses.

15   Q.    What software system does Michigan use today?

16   A.    The Michigan software system is one that is called

17         the -- give me just a second.  Changing states.  It's

18         called the Qualified Voter File database or QVF.

19   Q.    And is QVF a vendor in this space?

20   A.    No.  QVF is custom software for the state.

21   Q.    So Michigan decided to build its own software for

22         voter registration database?

23   A.    That's right.

24   Q.    You indicate that the attacks could cause voters to

25         receive the wrong ballot or be prevented from casting

J.  Alex Halderman , Ph.D.                    February 25, 2020
Fair Fight Action, Inc., Et Al. Vs. Raffensperger, Brad, Et Al.

Page 120

1           a regular ballot.  Are you familiar with the

2           provisional balloting process?

3     A.    I am.

4     Q.    And if there was an attack like the attack you're

5           describing in 23(a), you'd expect to see an increase

6           in provisional ballots for people who weren't in the

7           registration database, right?

8     A.    That's probably right.

9     Q.    Are you aware if there's been such an increase in

10          Georgia from 2016 to 2018?

11    A.    I don't know.

12    Q.    You indicate that they could also be used to steal

13          information that could be used to impersonate voters.

14          You're aware that Georgia has a photo ID requirement

15          for voting?

16    A.    I am.  But that doesn't apply to absentee by mail.

17    Q.    So your reference to voter impersonation here refers

18          to absentee by mail impersonation, not in-person

19          impersonation?

20    A.    Not in-person impersonation.

21    Q.    Which is much more of a tongue twister than I

22          realized it was going to be.

23    A.    That's right.  Absentee by mail or to access voter

24          registration records.

25    Q.    The second type of attack that you propose, attackers

J.  Alex Halderman , Ph.D.                    February 25, 2020
Fair Fight Action, Inc., Et Al. Vs. Raffensperger, Brad, Et Al.

Page 121

1          could sabotage polling place equipment and prevent

2          them from functioning on election day.  Do you have

3          any evidence that any sabotage of polling place

4          equipment that kept it from functioning has happened

5          in Georgia?

6     A.   No.  Although, the new equipment has only been in use

7          for a very short period of time.

8     Q.   Do you have any knowledge of the physical security

9          requirements for state election board rules

10         surrounding the new system?

11    A.   I haven't reviewed them in detail.

12    Q.   And I'm assuming you haven't visited any counties to

13         review their inspection of how they're maintaining

14         the election equipment.

15    A.   No.  Although, I have -- I'm familiar with reports

16         from others who have visited Georgia counties in the

17         past and have seen some of the physical security

18         mechanisms in place.

19    Q.   And was that before or after the purchase of the new

20         system?

21    A.   That was before the purchase of the new system.

22    Q.   So today you don't know what physical security

23         requirements might be available to mitigate an attack

24         outlined in 23(b); is that right?

25    A.   23(b) is referring not specifically to attacks that

Page 122

1        require physical security compromise, but ones that

2        involve compromise of the software and data running

3        in the system by any means, including by remote

4        cyberattack.

5   Q.   Okay.  So it's your testimony that the Dominion

6        system is subject to remote cyberattack that could

7        compromise its functioning?

8   A.   Potentially, yes.

9   Q.   You say at the end of that that the attacker could

10       target such sabotage at jurisdictions that strongly

11       favor a particular candidate and cause a partisan

12       shift.  You don't have any evidence that that's ever

13       happened in Georgia, do you?

14  A.   No, I don't.  Though, again, the system has only been

15       in use a few weeks.

16  Q.   23(c), you talk about the manipulation of optical

17       scanners or EMS systems to report fraudulent

18       outcomes.  Do you have any evidence that's ever

19       happened in an election in Georgia on the new system

20       or any system?

21  A.   No, I don't.  Although, the new system is new.  And

22       the old system, I don't think anyone has ever done

23       the kind of analysis of the optical scanners and EMS

24       servers that would be required in order to make a

25       strong statement about whether it had happened.

Page 123

1    Q.    You reviewed the GEMS databases for the state's old

2          system, though, correct?

3    A.    Yes, I have.

4    Q.    Have you discovered any malware compromise in that

5          review?

6    A.    No.  But the GEMS databases themselves are no

7          substitute for reviewing the actual software running

8          and installed on the servers.

9    Q.    But you don't know if anybody has undertaken that

10         kind of review in the last six months, say?

11   A.    No, I don't think so.

12   Q.    You indicate that at 23(c), attack could alter all

13         digital records of the election results.  And that's

14         where, again, you're coming back to the rigorous

15         manual audit or a recount of the paper ballots.  Then

16         you say, Georgia law doesn't currently require that.

17         What is your understanding of what Georgia law does

18         require?

19   A.    So my understanding of what Georgia law requires is

20         that it requires an audit this year but not a risk

21         limiting one.  It requires an audit pilot by the end

22         of 2021.  And that after that, the requirement

23         depends on the outcome of the pilot.

24   Q.    And you don't know what Georgia's current plans are

25         related to auditing of ballots going forward on the

J. Alex Halderman , Ph.D.                    February 25, 2020
Fair Fight Action, Inc., Et Al. Vs. Raffensperger, Brad, Et Al.

Page 124

1         new system, correct?

2    A.   Auditing ballots on the new system.  My understanding

3         is that Georgia does not require -- does not

4         currently plan to require a rigorous audit.

5    Q.   Have you reviewed any state election board rules

6         related to audits in Georgia?

7    A.   I have reviewed some state board election rules

8         related to audits in Georgia, but I can't -- I'm not

9         prepared to tell you exactly what the -- which set of

10        rules those were.  I just don't remember.

11   Q.   Are you aware that Georgia is working with Verified

12        Voting on the development of its audit processes?

13   A.   I'm aware that they were -- that they have been

14        working together in the past.

15   Q.   And do you support that kind of collaborative effort

16        to develop audits for jurisdictions?

17   A.   Well, look, I support work to implement robust

18        audits, but you have to actually get there in order

19        to have the benefit.

20   Q.   Do you based on your expertise in the design of

21        audits believe that piloting audits is a helpful

22        practice before you implement a full audit procedure

23        in a jurisdiction?

24   A.   Yes, I do.  But you have to actually implement the

25        full audit procedure in the jurisdiction.

J. Alex Halderman , Ph.D.                    February 25, 2020
Fair Fight Action, Inc., Et Al. Vs. Raffensperger, Brad, Et Al.

Page 125

1    Q.    And the type of attack you outline in 23(c) is also

2          true of a hand-marked paper ballot system; is that

3          correct?

4    A.    Yes, that's correct.

5    Q.    In 23(d) you talk about an infiltration to sometimes

6          print ballots differing from a voter's onscreen

7          selections.  And it's basically (d) and (e), the way

8          I read them, are two types of attack, one that

9          changes only the bar code, one that changes the bar

10         code and the human readable text.  Again, you

11         indicate that a 23(d) attack must be rigorously

12         audited or else it could go undetected.  Is that a

13         fair statement?

14   A.    That's right.

15   Q.    And so it's your testimony that a sufficient audit

16         would mitigate against the 23(d) style of attack,

17         right?

18   A.    That's right.  But it would have to be an audit that

19         was more rigorous than any audit that I understand to

20         be planned in Georgia.

21   Q.    But you don't currently know what's being planned in

22         Georgia; is that right?

23   A.    Well, I know what's being -- what's been publicly

24         talked about in Georgia, and I told you what my

25         understanding of the legal requirement is.

Page 126

1    Q.    Have you ever seen a, and this is going to be in any

2          context, lab or otherwise, a virus or malware that

3          would alter only the ballot bar code on a Dominion

4          system?

5    A.    On a Dominion system, no, I have not.

6    Q.    Have you ever seen in the lab or otherwise a piece of

7          malware or virus that would alter both the bar code

8          and the human readable text on a Dominion system?

9    A.    No.  Although, on other systems I have.

10   Q.    In 23(e) when you say research shows that few voters

11         carefully review their printed ballots, you're

12         referring to the two studies you cite later in your

13         report; is that right?

14   A.    Yes, I am.

15   Q.    And no other studies beyond those?

16   A.    I'm referring to those two studies.

17   Q.    And you say that the fraud sufficient to change the

18         winner of a close race might go undetected.  One

19         thing I've always wondered about these kind of

20         possible scenarios is how would an attacker know what

21         will be a close race?

22   A.    Right.  So usually by pre-election polling is one way

23         that an attacker can potentially conclude that a race

24         is likely to be close.

25   Q.    And in races where there's not regular polling, for

Case 1:18-cv-05391-SCJ   Document 401-1   Filed 06/27/20   Page 129 of 243

J. Alex Halderman , Ph.D.                    February 25, 2020

Fair Fight Action, Inc., Et Al. Vs. Raffensperger, Brad, Et Al.

Page 127

1       example, smaller races, are there other methods

2       someone could try to use to determine what they would

3       need to alter?

4    A.    I'm sorry.  Can I actually turn this off?

5    Q.    Sure.

6                 (Recess taken.)

7                 THE WITNESS:  I'm sorry.  Can you

8          repeat your question, please.

9    BY MR. TYSON:

10   Q.    Sure.  So in a race that is a smaller jurisdiction

11       where there's not regular polling, for example, of a

12       race, state house race, county commission race, how

13       would an attacker go about determining what would be

14       a close race that they could try to throw in that

15       context?

16   A.    Well, they could cheat anyway just in case it's

17       close, right?  So they don't necessarily need to know

18       for sure that it's going to be close in order to

19       attempt an attack and succeed if it is, in fact,

20       close.

21   Q.    And then in 23(e) you indicate that no audit or

22       recount could detect that kind of attack because the

23       digital and paper records would be wrong.  And the

24       only way -- now this is me.  Is it correct that the

25       only way a 23(e) attack would be detected is if a

Page 128

1          sufficient number of voters carefully reviewed their

2          printed ballots?

3     A.   That's the only surefire way that such an attack

4          would be detected, and then also assuming that there

5          was a careful audit of the paper trail.

6     Q.   So the way I read this, the attacks you outline in

7          (c), (d), and (e) could be mitigated or detected by

8          sufficiently rigorous audits with voters carefully

9          reviewing their printed ballots in a sufficient

10         number.  Is that fair to say?

11    A.   I think that's fair to say.

12    Q.   And the attack outlined in (a) would be mitigated by

13         the use of provisional ballots, right, and possibly

14         detected through a spike in provisional ballots

15         there?

16    A.   Well, all right, wait a minute because it's -- it

17         matters a lot what we mean by mitigated.  That attack

18         in (a) would at least be detected as a result of a

19         spike in ballots.  But if it's already caused there

20         to be long lines or other chaos at the polling place,

21         there's no way that you can go back and fix it.

22    Q.   Okay.

23    A.   These other attacks in I think you said (c), (d), and

24         (e) were mitigated by a combination of voters

25         robustly verifying -- or rigorously verifying their

Page 129

1        ballots and a sufficiently robust audit.  Although

2        that's true, I don't think that there is any -- that

3        there is sufficient evidence to conclude that it's

4        possible to induce voters to rigorously verify their

5        ballots to the necessary level in an all BMD context.

6   Q.   And you made an important distinction.  So there are

7        methods by which (a), (c), (d), and (e) can be

8        detected, and then there will be at least some basis

9        to go and investigate further what actually happened.

10       Is that fair to say?

11  A.   So we have to -- we should probably make a diagram

12       about that or something like that to distinguish

13       exactly which circumstance detection versus

14       correction is possible.

15  Q.   Why don't we try it this way?  Under (a), you can

16       detect an attack outlined in 23(a) by a spike in the

17       provisional ballots for individuals not in the voter

18       registration database.

19  A.   Depending on which variation of this attack.  But for

20       plausible variations, I would agree with you.

21  Q.   And then for (b), I'm assuming that would be

22       relatively obvious because things are not working.

23       So that would be a very detectable type of attack?

24  A.   Yes.  Hard to recover from, but one that you know

25       chaos is happening.

Page 130

1    Q.    And (c) can be detected through a sufficiently robust

2          audit or a recount, correct?

3    A.    Yes.

4    Q.    And (d) can be detected through a sufficiently

5          rigorous audit.

6    A.    Yes.

7    Q.    And then (e) can be detected --

8    A.    Although, (d) cannot necessarily be corrected by a

9          sufficiently rigorous audit.

10   Q.    That's why I'm asking specifically just the detection

11         question for each of these.

12   A.    Yes.  Okay.

13   Q.    And then for (e), it can be detected through

14         sufficient number of voters carefully reviewing their

15         printed ballot and sufficiently rigorous audits.

16   A.    Yes.

17   Q.    Okay.  And in each of those scenarios, there would

18         then be a basis to conduct a further investigation to

19         find evidence of the types of attacks that have been

20         outlined, right?

21   A.    Well, it depends.  So in some of those scenarios,

22         it's too late.  The election has already been

23         disrupted.  In other cases, in other cases, if you

24         detect that something is wrong, you don't have any

25         information available by which to go back and correct

Page 131

1          the changes that have happened.

2    Q.    You're familiar, I'm assuming, with the process of an

3          election contest?

4    A.    Yes.

5    Q.    And so there already exists provisions in Georgia law

6          and I'm sure other states as well that if, for

7          example, people who were ineligible incorrectly vote,

8          there's a provision to handle that through an

9          election contest.  Are you aware of that?

10   A.    Yes.

11   Q.    And so you said it's too late in terms of, you know,

12         once we detect it.  But if we detect it and an

13         election contest is filed, the election can be

14         re-run, just like it would be if ineligible people

15         were voting, right?

16   A.    That's true.  I would hate it -- I would hate to be

17         Georgia if we have to re-run the 2020 presidential

18         election because of Georgia's voting system.

19   Q.    And it's your testimony that you don't have any

20         evidence that any of the attacks in (a) through (e)

21         have ever occurred in an actual election in the

22         United States, right?

23   A.    No.  But election systems in many jurisdictions in

24         the United States don't produce the kind of evidence

25         that we'd need in order to know that these attacks

Page 132

1          have happened.

2     Q.   In paragraph 24, you begin discussing malware,

3          malicious software that could be introduced into the

4          election equipment.  You don't have any evidence that

5          malware has been introduced into election equipment

6          in use in elections in Georgia, do you?

7     A.   No, I don't.  Although, to my knowledge, no one has

8          done the kind of forensics to any piece of election

9          equipment in Georgia that would be the most probable

10         way to detect such malware intrusion if it occurred.

11    Q.   And the list of introduction of methods of malware

12         introduction in 24, that's true in every state,

13         correct?  You could introduce malware if you had

14         these types of things into optical scanners, for

15         example, in every state system or election management

16         system?

17    A.   Yes.  That is true.

18    Q.   In paragraph 25, you begin with a little bit more

19         detailed discussion of the pieces connected to the

20         internet.

21    A.   Could we maybe take a break at some point soon?

22    Q.   Certainly.  I'm fine to take a break now, if you'd

23         like to.

24    A.   All right.  If we could.

25    Q.   Absolutely.  Thank you.

Page 133

1              (Recess taken.)

2    BY MR. TYSON:

3    Q.    So turning to paragraph 25, we talk about some

4          components oven the system that are directly

5          connected to the internet.

6    A.    That's right.

7    Q.    Now, we've discussed a little bit the MVP and OVR

8          systems.  What is your understanding of how the MVP

9          system is connected to the eNet database?

10   A.    Well, let me see if I can remember for this

11         specifically for the MVP.  The MVP -- the MVP I know

12         receives information from the eNet database and I

13         believe contains a way to update that information.

14         But that may be in the OVR system.  It's been a while

15         since I've looked at them independently.

16   Q.    And so the OVR system, do you understand how that is

17         connected with the election system?

18   A.    Well, it generates voter registration requests that I

19         understand have to be reviewed by a person, but that

20         data then is fed into the database.

21   Q.    And are you recommending that no voter registration

22         information be put online for security purposes?

23   A.    No.  But what I'm recommending is that especially

24         heightened security precautions should be taken for

25         the components that are online because they create a

Page 134

1        path by which an attacker could potentially come from

2        anywhere in the world and access the system.

3    Q.   In the third sentence of paragraph 25, though, the

4        criticism seems to be just that they are connected to

5        the internet.

6    A.   This isn't a criticism.  This is an expression of --

7        an expression of the nature of the risk.

8    Q.   And so this is a risk that there's at least a good

9        policy reason to encounter because we want voters to

10       have information about their voting information?

11   A.   Perhaps.  And it's a risk that -- but it's also a

12       risk that is especially heightened in Georgia due to

13       the nature of the problems that have already been

14       detected in the eNet system and the reviews that have

15       happened so far.

16   Q.   You don't have any evidence that Georgia's eNet

17       system has been directly targeted by malicious

18       actors, do you?

19   A.   Just the broad conclusion of the Mueller

20       investigation and the Senate Intelligence Committee

21       that Georgia was among the states whose systems were

22       targeted by Russia in 2016.  And I think it's a

23       inference that the online components of the

24       registration system were among those targeted.

25   Q.   Do you know how Georgia maintains backups of its eNet

Page 135

1       registration system or if it does?

2   A.  I believe it does, but I don't know the specifics

3       about how those backups are maintained.  And it's a

4       good thing that it does.

5   Q.  In paragraph 26, you talk about components that are

6       not connected to the internet that could be targeted.

7       And one of the ways is removable media.  And you cite

8       the Stuxnet computer virus.  Are you with me on that?

9   A.  Yes.

10  Q.  And it's your testimony that that was attacked

11      through removable media and not through programming

12      at the manufacturer?

13  A.  Stuxnet was designed to, among other things, spread

14      through removable media.

15  Q.  Did the initial infection of Stuxnet come through

16      removable media?

17  A.  I think I've seen conflicting reports and conclusions

18      about that, but the way that the Stuxnet malware was

19      designed was able to spread to disconnected systems

20      by a removable media.

21  Q.  And in the next sentence you say that attackers could

22      employ this method to infect state or county EMS and

23      spread from there to scanners and BMDs when workers

24      program them for the next election.  Do you have any

25      evidence that this has ever happened to a Dominion

J. Alex Halderman , Ph.D.    February 25, 2020
Fair Fight Action, Inc., Et Al. Vs. Raffensperger, Brad, Et Al.

Page 136

1        system?

2    A.    No, I do not.  Although, the Dominion system is very

3          new.

4    Q.    So let's talk about the Dominion system.  That leads

5          up to paragraph 27.  And your opinions in this

6          section about the Dominion components, I think we've

7          discussed, came from your review of the technical

8          documentation, the California and other evaluations

9          of it, not from your personal review, correct?

10   A.    That's correct.  They're based on my experience with

11         other similarly designed voting systems as well.

12   Q.    Now, you in paragraph 27 say, Dominion does not

13         dispute that its devices can be hacked by

14         sufficiently sophisticated adversaries.  And that's

15         not really that remarkable of a statement, is it?  I

16         mean, can't any computer, we've already discussed, be

17         hacked by sufficiently sophisticated adversaries?

18   A.    I think that's actually a critically important point

19         because this is the entire reason that we need the

20         paper trail, the paper trail to reflect accurately

21         voters' intentions and the paper trail to be

22         rigorously audited.

23   Q.    So you would agree that that's not really a

24         remarkable statement, though, because it's a computer

25         that can be hacked, which is basically every

Page 137

1         computer?

2    A.   I agree that it's basically every computer that can

3         be attacked.  But again, that's really a core part of

4         why Georgia even has a new voting system right now,

5         that all computer systems can be hacked, and we need

6         to be very, very careful to make sure that, you know,

7         voting system context, the correct outcome is going

8         to be determined even if the systems are successfully

9         attacked.

10   Q.   The first reason you cite, you say one reason why

11        this is true.  So you're going to give, I guess, a

12        couple of reasons why it can be hacked.  I guess

13        isn't the first reason why it's true is because it's

14        a computer?

15   A.   I suppose so.

16   Q.   Okay.  You first cite the complexity of the software,

17        though.  Have you compared Dominion's software with

18        the number of source code lines in other BMD systems?

19   A.   In other voting systems.  Not -- I'm not sure it's

20        specifically in other BMD systems.

21   Q.   And is it your testimony that the number of lines of

22        code is higher in the Dominion system than other

23        voting systems?

24   A.   It's ten times as much code as Georgia's previous

25        voting system.

J.  Alex Halderman , Ph.D.                    February 25, 2020
Fair Fight Action, Inc., Et Al. Vs. Raffensperger, Brad, Et Al.

Page 138

1    Q.    And compared to other ballot marking device systems?

2    A.    I don't know.  It's probably similar, but I can't --

3          I can't estimate exactly how much.  Probably -- yeah.

4          I can't estimate how much.

5    Q.    The ICP scanner you indicate has 475,000 lines of

6          source code.  The ICP scanner is the optical scanner,

7          right?

8    A.    The precinct-based optical scanner as opposed to the

9          central count.

10   Q.    And is that similar to the number of lines of code

11         for other precinct-based scanners you've evaluated?

12   A.    It's more code than for other precinct-based scanners

13         that I've evaluated by something like a factor of

14         three or four.

15   Q.    And you indicate that the software is written in

16         C/C++, and you say that that programming language is

17         particularly susceptible.  Is that true of all

18         software written in C/C++, that it's more vulnerable

19         than other software?

20   A.    It's extremely difficult to write software in C and

21         C++ that is even reasonably secure to the point that

22         I'm advocating that my department stop teaching those

23         programming languages to undergrads.

24   Q.    Are those programing languages used in commercial

25         applications today?

Page 139

1    A.    They are.  Although, decreasingly so because of the

2          security risks.

3    Q.    And the security risks on the C, C++ front on the

4          precinct scanner are there for hand-marked paper

5          ballot systems too, correct?

6    A.    Yes.  That's part of the reason that the system needs

7          to be audited.

8    Q.    You say in paragraph 29 that software the size and

9          complexity of Dominion code inevitably has

10         exploitable vulnerabilities.  So is it true then that

11         just having a large number of lines of code always

12         leads to exploitable vulnerabilities?

13   A.    In practice, yes.

14   Q.    The quote at the end of 29 from the California study,

15         if the system were secure, it would be the first

16         computing system of this complexity that is fully

17         secure.  Would you ever categorize any computing

18         system as fully secure?

19   A.    There are some simple computer systems for which you

20         could plausibly make such a statement, but they're

21         very simple computing systems.

22   Q.    Like an Atari-level computing system?

23   A.    Probably not even that.

24   Q.    And so when you reference nation state attackers in

25         29 discovering and exploiting novel vulnerabilities

Page 140

1          in complex software, that basically is pretty much

2          every piece of software has exploitable

3          vulnerabilities, right?

4     A.   That's right.  It's another way of saying that if the

5          Russian government decides to target Georgia's

6          elections in 2020, they're likely to succeed.

7     Q.   And ultimately, that's not a function of a Dominion

8          system, a function of the lines of code.  It's just a

9          function of it being a computer that's programmed by

10         software, isn't it?

11    A.   And a function of the lack of things like a

12         strongly -- a paper trail that voters -- a paper

13         trail that we can be sure reflects voter intent even

14         in the face of attack and a question of whether there

15         is a rigorous enough audit.

16    Q.   And so essentially it's your testimony that there is

17         no way we can ever secure any computerized voting

18         system adequately, which is why you advocate for a

19         hand-marked system primarily?

20    A.   I'm not opposed to the use of technology in voting in

21         general, but that technology has to be used in ways

22         where we don't have to trust that the technology is

23         functioning correctly in order to be sure the

24         election outcome is right.

25    Q.   But you would never place a piece of technology

Page 141

1           between a nondisabled voter and the ballot?

2    A.    I think it's unwise to do that if there were

3           alternatives, and hand-marked paper ballots are such

4           an alternative.

5    Q.    In paragraph 30, you talk about using outdated

6           off-the-shelf software modules.  Isn't that a

7           relatively common practice when designing software?

8    A.    It's actually not a common practice among

9           well-written software.  Well-written software today

10          tends to use automated methods to make sure that the

11          dependencies are up to date.

12   Q.    And so when we discussed earlier the use of

13          open-source software and off-the-shelf hardware,

14          you're saying it's not a good idea to use

15          off-the-shelf software; is that fair?

16   A.    I'm saying if you're going to use off-the-shelf

17          software, you have to make sure that it's up to date

18          every time that you're shipping a new version of your

19          product and you have to ship a new version of your

20          product every time there's security updates to those

21          downstream dependencies.  That's a critical part of

22          the modern software development, of modern software

23          development practices that isn't reflected in the

24          Dominion system.

25   Q.    And every EAC-certified system has to have its

J.  Alex Halderman , Ph.D.                    February 25, 2020
Fair Fight Action, Inc., Et Al. Vs. Raffensperger, Brad, Et Al.

Page 142

1          software certified and maintained by the EAC; is that

2          correct?

3     A.    Tautologically every EAC-certified system has to have

4          its software certified.  That's right.

5     Q.    And the certification process includes the EAC

6          maintaining a gold disc of that version of the

7          software that is the certified version; is that

8          correct?

9     A.    That -- essentially, yes.

10    Q.    And so any time a software manufacturer wishes to

11         make any change, including a security update, they'd

12         have to get their software recertified by the EAC,

13         right?

14    A.    That's part of the problem with the Georgia voting

15         system, that, in fact, its software is out of date

16         because a new version -- if there were security

17         updates needed, they're likely going to have to go

18         through further certification before they can be

19         used.

20    Q.    So that's a yes, it has to be recertified if there's

21         changes for security?

22    A.    It depends on quite what the changes are.  But

23         sometimes it has to go through a complete

24         recertification.

25    Q.    In paragraph 31 you say, outdated software components

J.  Alex Halderman , Ph.D.                    February 25, 2020
Fair Fight Action, Inc., Et Al. Vs. Raffensperger, Brad, Et Al.

Page 143

1          are a security risk because they have these

2          documented vulnerabilities, and you cite, for

3          example, a list of 254 known vulnerabilities.  Is a

4          vulnerability always an exploitable vulnerability?

5          How are you using the term vulnerability in this

6          paragraph?

7     A.   Whether it's exploitable or not in this context

8          depends on what the -- depends on the specifics of

9          the particular problem and what the attacker is

10         trying to do.

11    Q.   So the fact that an Android operating system has 254

12         known vulnerabilities is just like saying it's a

13         piece of software, right, because every software has

14         vulnerabilities?

15    A.   Well, no, not exactly.  The problem is that it's a

16         much stronger statement than simply it's a piece of

17         software.  This is a piece of software that's already

18         been analyzed, people understand where many of the

19         vulnerabilities are, and I can provide a recipe to

20         make it even easier for an attacker to get in or to

21         allow less sophisticated attackers to successfully

22         compromise the system that don't have the resources

23         of a nation state.

24    Q.   So the fact that there are 254, does that tell you

25         anything about the relative risks of the use of this

Page 144

1          particular version of Android?

2     A.    As compared to --

3     Q.    In the election contest, I should say.

4     A.    As compared to newer versions of Android?

5     Q.    As compared to anything.  Does the fact of the number

6          of known vulnerabilities tell you how vulnerable a

7          piece of software actually is?

8     A.    It's a good indicator.  It's certainly an indicator

9          of the level of vulnerability.  And 254 unpatched

10         vulnerabilities is a very bad situation to be in.

11    Q.    And is that number higher or lower than the number of

12         known vulnerabilities in other BMD systems?

13    A.    I don't know the number of known vulnerabilities in

14         other specific BMD systems off the top of my head,

15         but I can tell you that in absolute terms that's

16         pretty high.

17    Q.    Your next paragraph, 32, talks about a cheap security

18         officer position that was vacant.  How is this

19         paragraph 32 informing your analysis of the relative

20         risk faced by Georgia?  And the reason why I ask that

21         is, from our discussions so far, it sounds like it's

22         a piece of software, it's a computer, it's going to

23         be vulnerable.  How is the existence or not of a

24         chief security officer informing your analysis?

25    A.    Well, this is informing whether Dominion is following

J. Alex Halderman , Ph.D.                    February 25, 2020
Fair Fight Action, Inc., Et Al. Vs. Raffensperger, Brad, Et Al.

Page 145

1          best practices in its security and its software

2          development and maintenance.  And not having a chief

3          security officer in place, I think is a sign of a

4          general -- is a sign of a general perhaps difficulty

5          in achieving security best practice.

6     Q.   So are you opining that Dominion does not take

7          security seriously?

8     A.   That the position is still vacant does not speak

9          highly of Dominion's security posture.  I'm opining

10         that there is -- that this is -- that this is a sign

11         of lax security practice.

12    Q.   And it's your testimony that the Dominion software is

13         not secure software, right?

14    A.   Yes.

15    Q.   And it's also your testimony that every ballot

16         marking device software is not secure software,

17         right?

18    A.   It is my testimony that no ballot marking device is

19         likely to be able to withstand a sophisticated nation

20         state attack, and that's why it's so important that

21         we have -- that all jurisdictions practice -- that

22         all jurisdictions -- that's why it's so important

23         that ballot marking devices be -- that the scope of

24         use of ballot marking devices be limited.

25    Q.   And you haven't done a full comparison of every

Case 1:18-cv-05391-SCJ   Document 401-1   Filed 06/27/20   Page 148 of 243
J. Alex Halderman , Ph.D.                February 25, 2020
Fair Fight Action, Inc., Et Al. Vs. Raffensperger, Brad, Et Al.

Page 146

```
 1        ballot marking device that's currently available,

 2        right?

 3   A.   That's right.

 4   Q.   And you haven't asked Dominion who has responsibility

 5        for security development and implementation of

 6        security in Georgia?

 7   A.   No, I haven't.  It's unclear who, if anyone.

 8   Q.   In paragraph 33 you say, Georgia certified the system

 9        without performing its own security testing or source

10        code review.  The system Georgia used is certified by

11        the EAC, right?

12   A.   Yes.  So were versions of Georgia's old system.

13   Q.   And part of the EAC's review for certification

14        involves security, correct?

15   A.   A very limited kind of security testing

16        unfortunately.  It's not rigorous.

17   Q.   So it's your testimony a state can never rely on EAC

18        certification for cybersecurity issues?

19   A.   I think it would be very foolish to rely only on the

20        EAC certification for security.  That's right.

21   Q.   In beginning of paragraph 34 we begin a walk through

22        the California test, which is a different version

23        than the version used in Georgia, right?

24   A.   It's a more recent version.

25   Q.   And I believe we've already covered this.  But you
```

Page 147

1    weren't involved in any of the California review of

2    the Dominion system, right?

3  A.  No, I was not.

4  Q.  You say in paragraph 35 that, like all security

5    testing, California's tests were necessarily limited

6    and could not be expected to find all exploitable

7    vulnerabilities.  Can you tell me about what you mean

8    by that sentence?

9  A.  Right.  So security testing -- security testing can

10    expose the existence of vulnerabilities.  It can't in

11    general prove that systems have no vulnerabilities.

12  Q.  So you can't prove a negative basically.  I can't

13    prove there are no vulnerabilities?

14  A.  Not with the normal means of security testing.

15  Q.  And is that why the security testing is necessarily

16    limited in scope, because it's just not possible to

17    find everything?

18  A.  Well, in part.  And there's also a question of the

19    rigor involved.  For instance, the California

20    top-to-bottom review of the -- in 2007 of the

21    equipment that Georgia has just gotten rid of spent

22    something like a man year of effort per system doing

23    code review, right, a very high level, an intensive

24    level of review.  Security testing of the kind I

25    understand that California does now, it's a much more

J. Alex Halderman , Ph.D.                     February 25, 2020
Fair Fight Action, Inc., Et Al. Vs. Raffensperger, Brad, Et Al.

Page 148

1           limited time and scale.  There's a quantifiable --

2           there's sort of a quantifiable difference as well.

3      Q.   So ultimately it's a policy decision how much effort

4           a state wants to put into its security testing.  Is

5           that fair to say?  California chose at one point to

6           do a massive amount of it.  Now it chooses to do

7           something less.

8      A.   I suppose you could characterize that as a policy

9           decision.

10     Q.   Would you characterize it as something different?

11     A.   No.  Again, I suppose you could characterize it as a

12          policy distinction.  I'm not sure I would

13          characterize it differently.

14     Q.   So in paragraph 35 you kind of distinguish the two

15          versions to say more recent versions of software tend

16          to contain fewer security vulnerabilities.  But you

17          haven't done any comparison, and to your knowledge no

18          one has, to know if that's the case, right, if

19          there's more or less vulnerabilities?

20     A.   Right.  Unfortunately, Georgia didn't do its own

21          security testing of a similar kind to California.  So

22          we don't have a direct comparison.

23     Q.   And you haven't -- I'm sorry.

24     A.   But in general, it's true that as software evolves,

25          vulnerabilities are corrected at a higher rate than

Page 149

1          they're introduced.

2   Q.    And you have not done any security assessment of

3         vulnerabilities in Georgia's Dominion system, right?

4   A.    No.  I haven't had the access to do that.

5   Q.    The next paragraph talks about the installation --

6         software installation files and a belief that it was

7         possible to inject things into the system.  And you

8         say, this implies that attackers could modify

9         Dominion installation files.  But I'm assuming you've

10        never tried to do that, right?

11  A.    No.  I have not had the access to try to do that

12        myself.  This is based on what California's testers

13        found.

14  Q.    And California's testers, again, looked at the

15        antivirus available.  Do you know if that same

16        antivirus is used in Georgia's system, or not?

17  A.    Yes, it is.

18  Q.    And you reference that the ballot marking device and

19        the precinct optical scanners have no antivirus

20        software at all.  Would you expect to find antivirus

21        software on a precinct scanner?

22  A.    Some precinct scanners can have antivirus software.

23        It depends -- it depends on the specific scanner.

24  Q.    And so are there particular manufacturers that

25        install antivirus software on precinct scanners?

Case 1:18-cv-05391-SCJ    Document 401-1    Filed 06/27/20    Page 152 of 243

J. Alex Halderman , Ph.D.                    February 25, 2020

Fair Fight Action, Inc., Et Al. Vs. Raffensperger, Brad, Et Al.

Page 150

1    A.    Yes.  So let me see.  No.  I can't -- I can't recall

2          off the top of my head.  But yes.

3    Q.    And so then the end of paragraph 37 you're saying,

4          malware that infected the Dominion components could

5          evade antivirus protection.  Again, that's possible,

6          but you don't know for sure, right?

7    A.    Well, with California's -- what California's test

8          found was, in fact, they tried to see if the

9          antivirus would detect malware samples, and in some

10         cases it failed to do that.  So that's the basis for

11         that conclusion.

12   Q.    And that was just specifically for the EMS server and

13         not for -- California didn't run those tests on the

14         BMD or the optical scanners, right?

15   A.    Well, the BMDs and optical scanners don't have

16         antiviruses.  So tautologically malware could evade

17         antivirus detection in those components.

18   Q.    And are you aware whether Georgia requires any other

19         components on the EMS server that would address

20         malware antivirus software different than California?

21   A.    I'm not.  But it would invalidate the EAC

22         certification for them to install such components.

23   Q.    So the EAC certification extends to the antivirus

24         components of the EMS server?

25   A.    Yes.

J.  Alex Halderman , Ph.D.                    February 25, 2020
Fair Fight Action, Inc., Et Al. Vs. Raffensperger, Brad, Et Al.

Page 151

```
 1    Q.    Paragraph 38 there's a discussion of physical access

 2          to a USB port.  And you say, this implies that no

 3          secret passwords or keys would be needed to exploit

 4          the problem, given physical access.  Isn't that a

 5          huge given under the circumstances that you don't

 6          know what physical access requirements exist for

 7          Georgia BMDs?

 8    A.    It's very difficult to have a physical access regime

 9          that would prevent any physical access under any

10          circumstances by an attacker.  So I think it's quite

11          significant that someone with physical access could

12          potentially alter the software running on these

13          devices.

14    Q.    If I gave you an unencrypted computer, physical

15          access to an unencrypted computer, no matter what

16          security measures I had on there, you could hack that

17          computer, right?

18    A.    Oh, definitely.

19    Q.    So doesn't physical access matter a lot then, the

20          protocols around physical access?

21    A.    The protocols around physical access are important.

22          But there's the question of, for instance, is the

23          computer actually encrypted.  If it is encrypted,

24          it's going to be more difficult to do something

25          hopefully for someone with physical access.
```

J. Alex Halderman , Ph.D.                    February 25, 2020
Fair Fight Action, Inc., Et Al. Vs. Raffensperger, Brad, Et Al.

Page 152

1    Q.    But ultimately since you were not aware of Georgia's

2          physical access and physical security requirements,

3          the statement in paragraph 38 doesn't really add much

4          to your analysis because we don't know what type of

5          physical access or what would be involved in someone

6          gaining physical access in Georgia, right?

7    A.    I'm not sure that I would agree with that.  I think

8          whatever the level of physical access protection that

9          Georgia has, the fact that given physical access

10         without any kind of secret information someone could

11         exploit the problem that the California reviewers

12         found creates significantly greater risks than if the

13         system had been designed without that problem.

14   Q.    So you say at the end of 39, these problems indicate

15         that the Dominion system was designed without

16         sufficient attention to security.  And so that's, I

17         guess, consistent with what you said previously.  You

18         don't believe there was any attention given to

19         secure -- sufficient attention given to security.

20         But ultimately, isn't it true that you find these

21         kind of vulnerabilities or problems with every

22         computer?  I guess what I'm trying to understand is,

23         you're opining about Georgia's Dominion system, but

24         really you're opining about ballot marking devices

25         generally.  I'm at a loss to see if you can never

J. Alex Halderman , Ph.D.                    February 25, 2020
Fair Fight Action, Inc., Et Al. Vs. Raffensperger, Brad, Et Al.

Page 153

1           sufficiently secure these systems, why is Dominion's

2           system any different than any other ballot marking

3           device being used today?

4      A.   So there are things that are true about all software

5           and all ballot marking devices, and there's further

6           evidence that these things are true about Georgia's

7           system specifically.  And, in fact, some of this is

8           what California's finding helps to suggest even more

9           specific recipes by which an attacker could strike

10          the Georgia Dominion system.  And this all gets back

11          to, once again, why the lack of sufficiently robust

12          audits and the universal use of BMDs for in-person

13          voters lead to such significantly heightened risks.

14     Q.   And that's true whether it's a Dominion system or any

15          other system if you're using BMDs for all voters,

16          right?

17     A.   Many of the same problems would in here.

18     Q.   And going to paragraph 40, ultimately California

19          chose to certify the Dominion system, right?

20     A.   They did.

21     Q.   And you know that they imposed much more stringent

22          security conditions than those in Georgia.  How do

23          you know that Georgia didn't adopt or utilize any of

24          the security conditions that California recommended?

25     A.   Based on -- based on my knowledge to date about what

J.  Alex Halderman , Ph.D.                    February 25, 2020
Fair Fight Action, Inc., Et Al. Vs. Raffensperger, Brad, Et Al.

Page 154

1           procedures, publically available procedures Georgia

2           has promulgated.

3    Q.     So the statement that California imposed

4           certification or more stringent security conditions

5           than those in Georgia is based on the Dominion

6           documentation you reviewed?

7    A.     Yes, in part.  In part on the California

8           documentation I reviewed, and in part on the overall

9           security posture of the Dominion system as used in

10          Georgia.

11   Q.     And you disagree with California's decision to

12          certify the Dominion system, right?

13   A.     In part.

14   Q.     What do you mean in part?

15   A.     In part.  I think the -- so the -- California,

16          because it has more stringent auditing requirements

17          than Georgia, faces somewhat less risk.  And

18          California does not -- most California jurisdictions

19          don't use the BMDs for all voters.  And in those

20          cases, they don't suffer from the same risks from

21          BMD-based attacks.  So I think the risk is less in

22          California than in Georgia.  I still think that

23          there's a risk in some California jurisdictions if

24          they're going to use BMDs for all voters.  But I

25          think the way that the system is used in most of

Page 155

1         California is less risky than Georgia.

2    Q.   Is it your opinion that a California county that uses

3         BMDs for all voters with these more stringent

4         security conditions has an acceptable level of risk?

5    A.   No.

6    Q.   So ultimately, even if Georgia agreed to every

7         security condition in California and imposed that for

8         all its BMDs, the fact that it's using BMDs for all

9         voters would be the thing that would -- that you

10        would say that's the security risk; is that right?

11   A.   Yes.  I think the BMDs for all voters, coupled --

12        they would need both the BMDs -- they would need both

13        sufficiently rigorous audits and not -- and to be

14        using BMDs for only a smaller fraction of voters in

15        order for the Dominion system with any set of

16        security precautions to be adequately safe.

17   Q.   So there is no situation where BMDs are used for all

18        voters, based on your current understanding of the

19        landscape, that you would say that was an appropriate

20        level of risk in an election system.  Is that right?

21   A.   I think that's probably safe to say.  Though, there

22        are matters of degree within that level of risk.

23   Q.   Which gets back to, I guess, our earlier discussion

24        about acceptable levels of risk.  Sitting here, do

25        you have a way by which you would determine the

J.  Alex Halderman , Ph.D.                    February 25, 2020
Fair Fight Action, Inc., Et Al. Vs. Raffensperger, Brad, Et Al.

Page 156

```
 1        acceptable level of risk for a BMD-for-all system?
 2   A.   Yes.  So in part, this is based on empirical
 3        observations about voters' likelihood of catching
 4        errors as in our January study, right?  And you can
 5        use that to estimate for a given BMD deployment and
 6        what fraction of voters are using it what -- how much
 7        evidence you would have of systemic error for a
 8        particular closeness of an election result.  That's
 9        one way of evaluating in a very quantifiable way the
10        relative risk.
11   Q.   And I apologize if I'm just not grasping the concept.
12        This is probably me, not you, so don't take this the
13        wrong way.
14   A.   It's probably me.
15   Q.   I just am trying to understand.  Ballot marking
16        devices for all voters is a scenario that you say
17        imposes a high risk such that it's too much risk.
18        You can point to the voters verifying at a level.
19        And so is it that if voters verified 90 percent of
20        their ballots, you would then say that's an
21        acceptable degree of risk for a BMD-for-all system?
22   A.   So the analysis is basically of the form, given this
23        fraction of voters using the system, is there -- is
24        it -- is it at all likely that election officials are
25        going to notice systematic fraud sufficient to change
```

Page 157

1          the outcome of a close election if attackers are able

2          to compromise the machines.  And if the answer is

3          yes, it's very likely, then that's probably an

4          acceptable risk.  If the answer is no, it's quite

5          unlikely, then that's an unacceptable risk.  So

6          there's some gray area in between, but we're not in

7          that gray area with Georgia's machines.

8     Q.   And when you say we're not in that gray area with

9          Georgia's machines, I know we're not for the voter

10         certification.  Are you saying the security

11         vulnerabilities alone take us out of the voter

12         verification question?

13    A.   No.  The overall posture of deployment takes us out

14         of the -- out of the gray area there.  That they are

15         used by all -- that they are used by all voters

16         unfortunately takes us out of that gray area.

17    Q.   So it is correct then that if BMDs are used for all,

18         we're out of the range of acceptable risk under any

19         construct?

20    A.   At least for BMDs that are available today.  It's

21         possible that future BMDs, some very different design

22         might result in different verifiability properties,

23         that voters would have a much easier time verifying

24         them.  Or perhaps someone will discover eventually a

25         way to get voters to reliably verify everything on

Case 1:18-cv-05391-SCJ    Document 401-1    Filed 06/27/20    Page 160 of 243

J. Alex Halderman , Ph.D.                    February 25, 2020

Fair Fight Action, Inc., Et Al. Vs. Raffensperger, Brad, Et Al.

Page 158

1          the ballot, but it seems extremely unlikely to me at

2          this point.

3     Q.   So let's move to voter registration database.  And

4          you talk about a cyber risk assessment of eNet from

5          two years ago.  Is that correct?

6     A.   That's right.

7     Q.   And I'm assuming you are relying on the publically

8          available information from the Curling case for

9          paragraph 41 and 42.

10    A.   Yes.

11    Q.   Okay.  You say that the PCC assessment or the

12         assessment of PCC software was limited in scope.  But

13         didn't we just say in 35 that all security testing is

14         limited in scope?

15    A.   This was particularly limited in scope.

16    Q.   Okay.  So too limited?

17    A.   It was particularly limited in scope.  The 2018

18         assessment, if I'm recalling correctly, was basically

19         just a functional assessment and didn't even get into

20         the inner workings of the code.

21    Q.   And you've not personally examined Georgia's security

22         environment for eNet or the software that Georgia --

23         or the eNet software itself in Georgia, correct?

24    A.   No.  Although, I'm familiar with the risk assessments

25         that Georgia commissioned in that environment.

J. Alex Halderman , Ph.D.                          February 25, 2020
Fair Fight Action, Inc., Et Al. Vs. Raffensperger, Brad, Et Al.

Page 159

1    Q.   In paragraph 42, you state that transferring the

2         operations does not mitigate the full range of

3         issues, and then you say the state has -- there's no

4         evidence the state has taken other steps to address

5         them.  What is your basis for that knowledge today?

6         This is -- you know, we're what, eight months past

7         the hearing where these issues were discussed.  Is it

8         your understanding that Georgia still has not

9         mitigated these?

10   A.   I'm aware of a -- I'm aware today of a very recent

11        status update in the Curling case where Georgia

12        asserts that it has taken some steps.  Although, I'll

13        note that update is devoid of sufficient technical

14        detail to have -- to conclude that the progress is

15        substantial.  It just says that some things have been

16        mitigated and others are still in process, which

17        based on previous testimony in the Curling case about

18        vulnerabilities that would have led someone to

19        believe that vulnerabilities were corrected in these

20        systems when they had not been corrected, I think

21        leaves me with significant reason for doubt.

22   Q.   You don't know sitting here today whether Georgia has

23        contracted with any cybersecurity vendor for any of

24        the more detailed security assessments that you

25        recommend, right?

Page 160

1    A.   I'm not sure.

2    Q.   And you don't know if Georgia's review of its

3         mitigation steps for the security assessment that

4         were outlined has been reviewed by its outside

5         cybersecurity vendors, do you?

6    A.   No, I don't.

7    Q.   And if all of those -- the full range of issues had

8         been fully mitigated, as recommended by the

9         cybersecurity vendor, would you have greater

10        confidence in the secure of Georgia's voter

11        registration database?

12   A.   I think it would also require further assessment and

13        source code review and mitigation of the things found

14        as a result of that before I would say I had further

15        confidence.  And the level of further confidence

16        would depend on the details of those analyses.

17   Q.   And those types of analyses cost money, don't they?

18   A.   Yes, they do.

19   Q.   In paragraph 43 you talk about attempts to infiltrate

20        the voter registration system.  And we've

21        discussed -- I think we discussed that piece already

22        about the internet connection.  But you say serious

23        vulnerabilities in the MVP website were discovered on

24        the eve of the November 2018 election.  What were

25        those serious vulnerabilities?

Page 161

1    A.    Yes.  So there were vulnerabilities in the websites

2          that would have allowed an attacker to access the

3          voter registration data of many individuals without

4          their cooperation or knowledge and that would have

5          allowed an attacker to access system files on the

6          server that were not intended to be exposed,

7          potentially critical components of the inner working

8          of the services.

9    Q.    Georgia's voter registration information about

10         identifying information on voters is public record,

11         isn't it?

12   A.    I don't believe that everything in the file is a

13         public record.

14   Q.    And you say in the next sentence, unauthorized

15         parties could have exploited these vulnerabilities to

16         access sensitive system configuration files and voter

17         registration data.  What's the basis for the

18         statement that they could have accessed -- I'm sorry.

19         I meant to ask about the next sentence.

20               This information would have allowed

21         attackers to fraudulently change voter registrations

22         through the OVR system.  What is the basis for that

23         statement?

24   A.    That the information contained in the My Voter Page

25         was sufficient to authenticate as a voter to the --

Case 1:18-cv-05391-SCJ    Document 401-1    Filed 06/27/20    Page 164 of 243

J. Alex Halderman , Ph.D.                    February 25, 2020

Fair Fight Action, Inc., Et Al. Vs. Raffensperger, Brad, Et Al.

Page 162

1    to the service that allows you to update your voter

2    information, like where you live.  And so it would be

3    possible for an attacker to use that information to

4    change the records of voters and cause them to be

5    registered in the wrong jurisdiction, for instance.

6  Q.  Is it your testimony that this type of attack could

7    have immediately updated the eNet system without

8    going through a registrar?

9  A.  No.  Although, I'm not sure that there is evidence

10   either that registrars would have spotted this attack

11   had it taken place.

12  Q.  And there's no evidence that this type of attack

13   occurred and that any registrations were ever

14   changed, correct?

15  A.  That's correct.  But I think it speaks to the level

16   of security preparedness of the voter registration

17   system.

18  Q.  Is it your understanding that the voter registration

19   system is at issue in this case?

20  A.  These are components of the voter registration system

21   by the definition used in basically every state.

22  Q.  And my question was, is it your understanding that

23   the voter registration system is at issue in the Fair

24   Fight Action case?

25  A.  Yes, I do understand that it is at issue.

J.  Alex Halderman , Ph.D.                    February 25, 2020
Fair Fight Action, Inc., Et Al. Vs. Raffensperger, Brad, Et Al.

Page 163

```
 1   Q.   Next we move to the electronic poll books in

 2        paragraph 44.  And we covered you have not personally

 3        reviewed the Poll Pad e-poll book, correct?

 4   A.   That's correct.  I'm relying on the information

 5        provided by Dominion, which included technical

 6        documentation for the Poll Pad and on the analyses

 7        done in other states and my expertise.

 8   Q.   Are you aware whether Georgia requires the wireless

 9        and internet capabilities of Poll Pads to be

10        disabled?

11   A.   I understand that it requires that during the process

12        of voting while polls are open, but that's -- that

13        the WiFi be disabled.  But I don't believe that it

14        requires that to be disabled at other points.

15   Q.   Do you know if Georgia has taken any steps to

16        permanently disable that access on Poll Pads?

17   A.   I don't know.

18   Q.   In paragraph 45, you discuss an attack to alter voter

19        registration data in the Poll Pads.  Are you aware

20        that Georgia requires paper records of all registered

21        voters in a precinct at each precinct?

22   A.   Yes, I suppose I do know that.

23   Q.   So if an attacker altered voter registration data or

24        disabled the Poll Pads, Georgia election officials

25        would have a way for voting to continue, correct?
```

Page 164

1    A.    To continue, although possibly at a much slower rate,

2          which could cause chaos on the ground.

3    Q.    But you haven't assessed what the rate of check-in

4          would be with a paper list versus an electronic list?

5    A.    I haven't.  But it's fairly easy to -- I think it's a

6          reasonable conclusion that it would be slower without

7          the use of the technology.

8    Q.    And so ultimately it was a policy decision Georgia

9          made to include technology for this purpose possibly

10         to speed up the check-in process?

11   A.    Or to decrease the cost of the check-in process.

12   Q.    You say in paragraph 46 that Georgia -- to your

13         knowledge, Georgia has not performed any security

14         testing of the Poll Pads.  It's possible they

15         performed that and you don't know, right?

16   A.    I suppose it's possible that they performed their own

17         testing and didn't tell anyone about it.  But that

18         would seem -- but I've been following the case with

19         the Georgia system carefully, and to my knowledge,

20         they have not.

21   Q.    Do you know if Georgia relied on the California

22         review when it made the selection or decided to go

23         with the Poll Pads?

24   A.    I don't know.

25   Q.    And in 47 you indicate that California conditionally

J.  Alex Halderman , Ph.D.                    February 25, 2020
Fair Fight Action, Inc., Et Al. Vs. Raffensperger, Brad, Et Al.

Page 165

1         certified the Poll Pads subject to 19 terms and

2         limitations.  Do you know if Georgia adopted any of

3         those terms and limitations?

4    A.   I don't know.  But one of the most important ones was

5         that the Poll Pad not be used to program or encode

6         smart cards that would interface with the BMDs, and

7         it's my understanding that Georgia has not adopted

8         that one.

9    Q.   And Pennsylvania also conditionally certified the

10        Poll Pad, right?

11   A.   That's right.

12   Q.   And they had some additional conditions and security

13        recommendations.  And you don't know if Georgia has

14        adopted those at any point in its implementation of

15        the Poll Pad, right?

16   A.   I don't -- I don't know.  Although, again, one of the

17        most important ones in Pennsylvania was the

18        prohibition on encoding smart cards from the Poll Pad

19        because that creates a path from the Poll Pad system

20        to the BMDs.  And Georgia does encode voter access

21        cards from the Poll Pad is my understanding.

22   Q.   If Georgia adopted all of the terms, limitations, and

23        security recommendations imposed by California and

24        Pennsylvania, would you still recommend against the

25        use of the Poll Pad?

J. Alex Halderman , Ph.D.                    February 25, 2020
Fair Fight Action, Inc., Et Al. Vs. Raffensperger, Brad, Et Al.

Page 166

1    A.    It would certainly further reduce the risk.

2    Q.    Would it reduce it to an acceptable level?

3    A.    Perhaps.  It's subject to -- subject to other

4          security conditions as well.  So that alone would not

5          necessarily be enough.

6    Q.    So when you say subject to other security conditions,

7          what other security conditions would it be subject

8          to?

9    A.    Well, I think it would take some time to do a full

10         analysis of that question.

11   Q.    And what process are you using to determine the

12         relative level of risk of the Poll Pads with and

13         without the California and Pennsylvania conditions,

14         or are you using one?

15   A.    So this is -- to determine the relative risk in that

16         case, this is what would -- what I'm doing to

17         determine that is modeling the different paths by

18         which an attacker might attempt to spread

19         infiltration through the voting system.  And so one

20         of the critical differences between the Georgia and

21         California and Pennsylvania models of using the Poll

22         Pad is the existence or not of this path from the

23         Poll Pads to the ballot marking devices.

24   Q.    In my hypothetical I asked you to assume that we

25         adopted all the Pennsylvania and California

J. Alex Halderman , Ph.D.                    February 25, 2020

Fair Fight Action, Inc., Et Al. Vs. Raffensperger, Brad, Et Al.

Page 167

1            conditions, which would include the prohibition on

2            that path.

3       A.   That's right.

4       Q.   How would you evaluate the level of acceptable risk

5            given the adoption of all those conditions?

6       A.   Well, I think it would involve a security analysis of

7            what the remaining modes of infiltration were and

8            what the -- what the full set of protection measures

9            allowed for or required in terms of a fail-safe.

10      Q.   And you haven't conducted that kind of analysis here,

11           right?

12      A.   Not in your hypothetical, no.

13      Q.   And you haven't conducted it as part of your report,

14           correct?

15      A.   I don't really need to in terms of this report

16           because the significant risk of the infection

17           spreading from Poll Pads to the BMD systems is

18           itself -- is itself the focus of my analysis here.

19      Q.   So the fact that items are being taken from the Poll

20           Pad to the BMD is a sufficient basis to determine

21           that is an unacceptable level of risk to encounter in

22           an election system, correct?

23      A.   That was sufficient to convince California and

24           Pennsylvania to prohibit that functionality entirely.

25      Q.   I'm --

Page 168

1    A.    I agree with that prohibition.

2    Q.    I just want to make sure I'm clear because you're

3          here opining that Georgia is taking an unacceptable

4          level of risk with its Poll Pads as well as part of

5          the structure of the election system.  Am I correct

6          about that?

7    A.    Yes.

8    Q.    And so what is the determination?  Is it the fact

9          that there's a card moving from the Poll Pad to the

10         BMD that makes it an unacceptable level of risk and

11         that distinguishes California and Pennsylvania, or is

12         there something else on which you're basing your

13         analysis that this degree of risk in using the Poll

14         Pads is unacceptable?

15   A.    So I'm basing that -- I'm basing that opinion on the

16         overall vulnerability of the Poll Pads and that

17         additional link between the Poll Pads and the BMDs,

18         and those are the primary -- that's the primary basis

19         for that assessment.

20   Q.    Okay.  And sitting here today, you can't say whether

21         or not California and Pennsylvania's use of the Poll

22         Pads is an acceptable or unacceptable level of risk;

23         is that correct?

24   A.    That's right.  I can't say that.  I haven't fully

25         evaluated that.

Page 169

1    Q.    Let's move next to supply chain threats.  You don't

2          have any evidence in paragraph 50 that attackers have

3          infiltrated the software development process of

4          Dominion KnowInk, PCC, or their suppliers, right?

5    A.    No.  I'm talking about the risk that that could

6          happen.

7    Q.    Right.  But you don't have any evidence it has

8          happened?

9    A.    I don't.  And I'm not sure that there would be such

10         evidence available if it had happened successfully.

11   Q.    And then in paragraph 51, you talk about the design

12         of several components overseas.  Is it your testimony

13         that Serbian programmers, that automatically means

14         that this is going to be accessed by the Russians or

15         influenced by the Russians in some way?

16   A.    No.  Not that it will automatically be, just that the

17         risk is even higher than if the software were

18         developed domestically in a facility that was not in

19         a location of a government closely aligned with

20         Russia.

21   Q.    And the EMS runs an antivirus software made by a

22         Czech company, you say, which earlier we said was the

23         Avast Antivirus file shield system; is that right?

24   A.    Avast, like a pirate.

25   Q.    And is Avast a widely-used antivirus software?

Page 170

```
 1    A.   It is.

 2    Q.   Why mention that it's a Czech company in that

 3         scenario?  Does that increase the risk if it's a

 4         widely-used piece of software?

 5    A.   It creates further risks because the -- although a

 6         widely-used piece of software -- although it is a

 7         widely used piece of software, it's still true that

 8         if attackers were to infiltrate that company, they

 9         could spread -- spread malicious functionality into

10         the election management system.

11    Q.   And so it's your testimony that the antivirus is both

12         a terrible system because it doesn't track stuff and

13         it grants this Czech company access to the server?

14    A.   It can be simultaneously true that it introduces new

15         risks and doesn't adequately mitigate other risks.

16    Q.   And your reliance for this section of your report is

17         from this Computer World article, right?

18    A.   I'm sorry.

19    Q.   I'm sorry.  Let me rephrase that.  In paragraph 51

20         the statement about Dominion using Serbian

21         programmers is based on this Computer World article,

22         correct?

23    A.   Yes.  Although, I'm aware that that has been reported

24         elsewhere.  I'm not sure where.

25    Q.   And this is a system that has been certified by the
```

Page 171

1              EAC since 2016, right?

2    A.     Yes.  Although, again, the EAC certification process

3           is not a -- it has significant limitations to its

4           security review.  It's not a rigorous security

5           review.

6    Q.     And your statement that a hostile government might

7           attempt to plant an agent at any of these companies,

8           black male honest employees, or hack into the

9           software development environments, that's true of

10          every election system and even ballot printing

11          services, right?

12   A.     I think it's an increased risk in foreign

13          jurisdictions, especially jurisdictions that are

14          aligned with potentially hostile governments.

15   Q.     So it's a true statement.  But you think that

16          Georgia's selection of Dominion led to an increased

17          risk of the -- of that sentence happening; is that a

18          fair statement?

19   A.     Yes.

20   Q.     And how are you evaluating the increased risk by

21          using foreign contractors versus domestic

22          contractors?

23   A.     This is -- well, it's just -- it's well known that --

24          it's well known among the -- among the -- in the --

25          it's well known in the study of supply chain risk

Page 172

1            that extra jurisdictional supply chains create

2            additional risks that are not -- that are more

3            greater in kind than the risks of domestically

4            produced and domestically sourced equipment.

5    Q.     So there's not a kind of scientific evaluation of

6           that.  It's just it is what it is, right?

7    A.     It's not quantified.  It's very difficult to

8           quantify.

9    Q.     Got it.  Paragraph 52, you say that the measures

10          being taken to safeguard are not sufficient, and then

11          you go through kind of some of these examples.  First

12          of all, the AuditMark process.  Have you ever done

13          research about how the AuditMark process works

14          specifically in Dominion software?

15   A.     I've reviewed Dominion's technical documentation

16          about it.

17   Q.     And in paragraph 54 you indicate that you have

18          designed malware that runs on an optical scanner that

19          can manipulate digital ballot images.  And that's

20          true of a hand-marked system or a ballot marking

21          device system, right?

22   A.     That's right.

23   Q.     And that was not in the Dominion system.  That was on

24          a different manufacturer; is that right?

25   A.     It works against Dominion-style ballots, among

Case 1:18-cv-05391-SCJ    Document 401-1    Filed 06/27/20    Page 175 of 243

J. Alex Halderman , Ph.D.                    February 25, 2020

Fair Fight Action, Inc., Et Al. Vs. Raffensperger, Brad, Et Al.

Page 173

1          others.

2     Q.   Have you tested it on Dominion's ICP and ICC

3          scanners?

4     A.   No.   But based on the way that the malware works, I

5          have no reason to doubt that it would function on

6          those scanners.

7     Q.   Would it take physical access to install the malware

8          on the scanners?

9     A.   No.

10    Q.   In paragraph 56 you indicate that the tampering

11         wouldn't be detected by the election software.   And

12         I'm assuming since that's not unique to BMDs.   This

13         is another reason why you urge audits because it

14         would be found in an audit, correct?

15    A.   It would be found in an audit that reviewed the

16         physical paper ballots as opposed to the digital

17         ballots, ballot images.

18    Q.   Do you know which method Georgia is going to use,

19         paper or digital images?

20    A.   So, again, this is talking specifically about

21         AuditMark itself as a mitigation, like the AuditMark

22         mitigation is insufficient -- sufficiently robust

23         audits, and I do believe that Georgia intends to do

24         its audits by going back to physical paper ballots,

25         could detect an attack like this.   The question is

J.  Alex Halderman , Ph.D.                              February 25, 2020
Fair Fight Action, Inc., Et Al. Vs. Raffensperger, Brad, Et Al.

Page 174

1           whether those audits are going to be sufficiently

2           robust.

3      Q.   And then the next section discusses hash comparisons,

4           and you say that Georgia may employ a method of hash

5           comparisons.  Do you know for sure whether or not it

6           will or not?

7      A.   I don't know for sure whether it will or not.

8      Q.   And hashing a value of a software versus a known good

9           hash value is used in a lot of computer security

10          contexts, correct?

11     A.   Yes.

12     Q.   And at the end of paragraph 60 you say that a

13          sophisticated attacker could conceal the presence of

14          malware even if officials practiced hash comparisons

15          according to Dominion's instructions.  Would a better

16          hash compare process be a more secure process?

17     A.   Potentially, yes.

18     Q.   Okay.

19     A.   Can we take a break sometime soon?

20     Q.   Sure.  Yeah.  We can go ahead and take a break now,

21          if you'd like to.

22     A.   Okay.

23               (Recess taken.)

24     BY MR. TYSON:

25     Q.   All right.  Dr. Halderman, you mention in paragraph

Page 175

1       61 -- I think we've already covered antivirus

2       software and end-point protection software provides

3       only a limited defense.  So it's your testimony no

4       matter what antivirus or end-point protection a BMD

5       or a precinct scanner had on it, that's not going to

6       protect them against a sophisticated nation state

7       attack, right?

8   A.  Yes.

9   Q.  In paragraph 62 you talk about one safeguard used in

10      Georgia is tamper-evident seals.  Are you aware of

11      those used on the new ballot marking devices?

12  A.  No, I'm not.  But I'm aware of fairly extensive

13      research on many different tamper-evident seals used

14      in different kinds of election systems, and none of

15      them offer strong security.

16  Q.  And so for physical security, your testimony is that

17      a tamper-evident seal is not going to provide any

18      real physical security; is that fair to say?

19  A.  No.  Not against a remotely capable adversary.

20  Q.  Would it provide some security against a locally

21      working adversary?

22  A.  Maybe against an adversary who didn't Google for how

23      to break the seals.

24  Q.  And so is there any value then to using seals on

25      voting equipment?

Page 176

1  A.  I don't say that there is no value to using seals,

2      but they don't protect against the kinds of attackers

3      that are at issue in -- in my report, which are ones

4      who are sophisticated hostile adversaries.

5  Q.  So there may be good reasons to use seals for just

6      kind of administration or documenting purposes, but

7      not to rely on those seals for purposes of protecting

8      against sophisticated attacks; is that a fair

9      statement?

10 A.  Yes.

11 Q.  And you have not reviewed the rules generally on

12     physical security or on the use of seals in Georgia

13     going forward, right?

14 A.  I have not seen those rules.

15 Q.  Okay.

16 A.  But this is generally true of seals used in voting.

17 Q.  Uh-huh.  And in considering other elements of

18     physical security, you didn't consider other elements

19     of physical security for Georgia ballot marking

20     devices, only seals in reaching your conclusions for

21     this report, right?

22 A.  I've considered what I've known about Georgia

23     physical security procedures in the past.  But if

24     they have been changed, then I'm unaware of what

25     other protections are in place.

J.  Alex Halderman , Ph.D.                    February 25, 2020
Fair Fight Action, Inc., Et Al. Vs. Raffensperger, Brad, Et Al.

Page 177

1    Q.    Next we call logic and accuracy testing.  Are you

2          aware what the logic and accuracy protocols are for

3          Georgia's new ballot marking devices?

4    A.    I'm not, but it doesn't matter.  No logic and

5          accuracy testing protocol is going to provide strong

6          protection against the kinds of attacks that I'm

7          discussing.

8    Q.    And you're not aware of any research that shows how a

9          piece of software could distinguish between a test

10         voter and an actual voter based on, for example, the

11         rate at which people vote; is that correct?

12   A.    It's certainly possible, and I've written malware

13         that attempts to do that.  And, in fact, our ballot

14         marking device study published in January discusses

15         some ways that malware could use different features

16         to try to distinguish between different categories of

17         voters, which I think touches on the subject of test

18         votes versus non.

19   Q.    And for parallel testing in paragraph 65, are you

20         aware of what Georgia's protocols are going to be for

21         parallel testing with the new ballot marking devices?

22   A.    I don't believe Georgia has made those public.  I'm

23         not aware.  But in general, it's impossible for

24         parallel testing to definitively or even reliably

25         detect misbehavior by a ballot marking device.

Page 178

1    Q.   And that's true even if at a random point in the

2         middle of the day every county went to every ballot

3         marking device and generated a certain number of

4         ballots?

5    A.   Yes.  Unfortunately it is true in that case.  And the

6         mathematical derivation is in the paper I cite.

7    Q.   You say at the end of paragraph 67, to your

8         knowledge, the state does not maintain sufficient

9         quantities of pre-printed ballots to allow voting to

10        continue under such a circumstance when the BMDs

11        fail.  Have you reviewed the state election board

12        rules regarding back-up ballots and what's required?

13   A.   I haven't reviewed them, but that's my understanding

14        from evidence that's come to light in the Curling

15        case about Georgia's current plans.

16   Q.   And do those include the changes that were made last

17        month to Georgia's rules regarding the number of

18        paper ballots?

19   A.   I don't know.  I don't know the timing.

20   Q.   So it's possible then that the state is now going to

21        require counties to maintain sufficient quantities to

22        allow voting to continue if the BMDs go out, and you

23        just don't know if that's the case, right?

24   A.   My understanding is that the -- the state plans to

25        have a very limited number of ballots available and

Page 179

1          to print more on demand, if necessary.  But the

2          problem is if all of the BMDs across a large region

3          were to be sabotaged, as is possible by a malicious

4          software spreading from say a county election

5          management system, then you'd have a simultaneous

6          failure and require a very large number of ballots

7          sufficient for all voters, which would be impossible

8          to produce on -- and distribute in time.

9    Q.    You say in the post-election audit portion that

10         officials could potentially detect certain kinds of

11         attacks by a rigorous audit of paper ballots.

12         Actually, before I get to that, that footnote at the

13         bottom of page 28, the Philip Stark paper.

14   A.    Yes.

15   Q.    Is that a peer-reviewed paper?

16   A.    I don't know whether he's had the paper since

17         peer-reviewed.  I have independently -- I have

18         assessed myself the correctness of the -- of Stark's

19         result, but I don't know if it's gone through formal

20         peer review or not.

21   Q.    So next we have sufficient audits.  And I think we've

22         talked through the various categories of how audits

23         can detect things already.  The good thing is we've

24         covered a lot of this, so I can move through here.

25                  All right.  So let's skip ahead to

Page 180

1          paragraph 72.  You say that the ballot marking

2          devices are computers, run outdated and vulnerable

3          software, must be programmed using the election

4          management system before every election.  This is --

5          kind of unlike DREs, this is an election system,

6          recommended by the National Academy of Sciences.  I

7          know that DREs were certified by the EAC -- certified

8          by the US Election Assistance Commission.  Why are

9          you taking the position that these are -- should

10         never be used by all voters in an election?

11   A.    Right.  So I'm taking that position based on

12         subsequent research that was called for by the

13         national academies in their study that has -- that

14         has established that the rate at which voters review

15         and catch errors in BMD-printed ballots is very low

16         and is, in fact, likely to be so low that an attack

17         on the BMDs in a close election wouldn't be detected

18         by election officials.

19   Q.    And so the subsequent research you're relying on are

20         the two studies about the rate of voter verification

21         of BMD ballots, right?

22   A.    That's right.  Although, there is previous work on

23         VVPATs systems that was highly suggestive that there

24         might well be a problem with BMDs.  So these new

25         results confirm and extend the problems with VVPATs

Page 181

1        to BMD-based systems.

2   Q.   And those prior studies with VVPATs were prior to the

3        National Academy of Science's recommendation, right?

4   A.   That's right.  But there was still at least some

5        substantial question about whether the findings would

6        apply with equal certainty or equal force to BMD

7        systems, but now there's now strong evidence that the

8        same problems occur.

9   Q.   All right.  So let's get to those two studies.  If

10       you want to jump ahead with me to paragraph 81.  So

11       the first study that you cite about the rate at which

12       voters verify or look at their ballot marking device

13       printed ballots was a study by Dr. DeMillo,

14       Robert Kadel, and Marilyn Marks; is that right?

15  A.   That's correct.

16  Q.   And you'd agree with me that Ms. Marks is an activist

17       for hand-marked paper ballots; is that a fair

18       assessment of her?

19  A.   Well, I'd agree that she's an election integrity

20       activist.

21  Q.   And she opposes electronic voting as a policy matter,

22       right?

23  A.   I'm not sure she opposes all electronic voting, but

24       she opposes paperless electronic voting.

25  Q.   Does she -- do you know, she opposes ballot marking

Page 182

1          devices for all people?

2     A.   I believe she does, yes.

3     Q.   And this study has not been peer-reviewed, has it?

4     A.   No, that study has not.

5     Q.   And when voters in the study spent only four seconds

6          reviewing their ballots, how many races were they

7          looking at, do you know?

8     A.   I don't know.  I don't know off the top of my head.

9     Q.   And do you know if that study evaluated the use of

10         signs or verbal cues or other things to ask voters to

11         verify their ballots?

12    A.   No.  That we evaluate -- that my research group

13         evaluated in the other study I cite.

14    Q.   So let's go to that one.  Paragraph 82 you have a

15         realistic simulated election.  Were the candidate

16         names in the election something that individuals

17         would recognize?

18    A.   Yes.

19    Q.   And what were the candidate names?

20    A.   The candidate names were the names of the candidates

21         from the most recent Michigan midterm.

22    Q.   Let me hand you what we've marked as 15.

23              (Exhibit No. 15 marked.)

24    BY MR. TYSON:

25    Q.   And is this your study with Mr. Bernard?

Page 183

1    A.    Yes.   And five other authors.

2    Q.    And Mr. Bernard is a student of yours, correct?

3    A.    Yes.   He's a Ph.D. student.

4    Q.    And have you found him to be reliable and a good

5          student?

6    A.    Yes.

7    Q.    Now, in the various scenarios that are outlined here,

8          you found that verbal prompting increased the number

9          of voters who were reviewing their ballots, correct?

10   A.    I did.

11   Q.    And you found that verbal prompting accompanied by

12         kind of identification of candidates on a slate

13         significantly increased the number of voters who

14         reviewed their ballots, right?

15   A.    Yes, it did.

16   Q.    And so in terms of a policy recommendation going

17         forward, is it your position that there is no way a

18         state can increase the number of voters verifying

19         their ballot marked device ballots based on your

20         research?

21   A.    The question is whether the increase is likely to be

22         significant enough that the state will have a high

23         chance of detecting attacks against a close election.

24         And the problem is that the magnitude of increase

25         that we found even with the best verbal prompts was

Page 184

1       relatively small.  And the magnitude, though, larger

2       that we found with the use of slates only applies to

3       the subset of voters who actually use slates.  So

4       unless use of slates can be the vast majority of

5       voters, even under the best of conditions, that

6       mitigation would not result in a high probability of

7       detecting attacks on close elections.

8   Q.  And this is the first peer-reviewed study of its

9       kind, studying this specific question of voter

10      verification and ballot marking devices, right?

11  A.  Yes.  Though I understand there are others now under

12      review that will be published soon.

13  Q.  And are you aware whether Georgia requires poll

14      workers to give verbal prompts to voters?

15  A.  I know that Georgia law requires signs, which we find

16      are not effective.  There may -- I don't know if

17      there are recently issued rules that also require a

18      verbal prompt.

19  Q.  So if the state election board issued rules requiring

20      a verbal prompt, that would at least move up the

21      chain a little bit in terms of verification, right?

22  A.  It would likely move it up.  But again, the rate

23      that -- the rate that would be required in order to

24      cause a significant -- excuse me.  In order to have a

25      high likelihood of detecting fraud even in close

Page 185

1      elections is something like ten times the improvement

2      that we measured in the study from verbal prompts

3      alone.  So there's a lot more work that would need to

4      be done or a lot more increase that would be needed

5      in addition to verbal prompts.

6   Q.  But ultimately it's fair to say that the study found

7      that a well-designed procedure can have a significant

8      impact on the rates of voters checking their ballots,

9      right?

10  A.  Significant in the sense of statistically significant

11      or reliably measurable, but not necessarily in terms

12      of adequate.

13  Q.  And the paper also concludes that more research is

14      needed in this area.  Do you agree with that, right?

15  A.  I do.

16  Q.  And you welcome additional research on this topic?

17  A.  I do.

18  Q.  And if you -- if that later research demonstrates

19      that voters check their ballots at a high enough

20      rate, as you've outlined in this paper from a

21      mathematical perspective, would that change your view

22      of the use of ballot marking devices?

23  A.  Yes.

24  Q.  You opine in paragraph 87 that election officials are

25      unlikely to take disruptive actions unless there's a

Page 186

1          certain or a fraction of BMD voters that are

2          reporting problems.  What are you basing the fact

3          that election officials are unlikely to take

4          disruptive actions on?

5     A.   In part the fact that there are a certain number of

6          reports of problems and inconsistencies in every

7          election.  And so election officials don't as a

8          general rule say we're going to have to take all of

9          our machines aside and study them just because there

10         was some sporadic reports of problems that could be

11         explained away by other things.  The rate would have

12         to be elevated in a way that stood out and was

13         unmistakable in order to take drastic action.

14    Q.   And your issue focused particularly on the margin of

15         victory being relevant to this consideration, right?

16         The analysis, the mathematical analysis.

17    A.   I'm sorry.

18    Q.   Let me rephrase that question.  In determining the

19         mathematical analysis you outline in this report, the

20         margin of victory was significant, right?

21    A.   Yes.

22    Q.   And so in a larger margin of victory, would that mean

23         fewer voters would have to report a problem?  Where

24         does the scale go in terms of larger margin of

25         victory versus smaller margin of victory?

J. Alex Halderman , Ph.D.                    February 25, 2020
Fair Fight Action, Inc., Et Al. Vs. Raffensperger, Brad, Et Al.

Page 187

1    A.    I see.  If the margin of victory is smaller, then

2          it's easier to attack the system, if that's the --

3          the question you're asking.

4    Q.    Yeah.  Thank you.

5    A.    It takes us back to the election official's prayer,

6          please let it not be close.

7    Q.    That's right.  And the election lawyer's prayer

8          usually as well.

9    A.    And the election security researcher's prayer.

10   Q.    Okay.  Paragraph 88.  Now we get to the question of

11         the DREs.

12   A.    I'm sorry.  Paragraph --

13   Q.    We can put aside the exhibit.  Yeah.  Exhibit 15 is

14         finished.  So paragraph 88 of your report.

15   A.    Okay.

16   Q.    We move to the DRE machines, correct?

17   A.    Yes.  Okay.

18   Q.    And you're aware DREs are never going to be used in

19         Georgia again, right?

20   A.    Yes.  Thank goodness.

21   Q.    And those were decertified by the Secretary of State

22         at the end of 2019?

23   A.    That's right, as my research suggested in 2006.

24   Q.    And you state at the bottom of 88 that the DRE system

25         was highly susceptible to cyber attacks.  But as

J.  Alex Halderman , Ph.D.                    February 25, 2020

Fair Fight Action, Inc., Et Al. Vs. Raffensperger, Brad, Et Al.

Page 188

1           we've discussed, there's no evidence that any of the

2           DREs in Georgia were ever actually compromised,

3           right?

4    A.     That's right.  But again, I don't think anyone has

5           ever actually inspected the software running in any

6           of those DREs.

7    Q.     And you cite the broad scientific consensus about

8           DREs not providing adequate security and you cite to

9           the Securing the Vote from the National Academy of

10          Science's report, right?

11   A.     Yes.

12   Q.     But you don't rely on that report for its

13          recommendations about ballot marking devices because

14          of the subsequent reports we've discussed, right?

15   A.     That's right.  The science about ballot marking

16          devices has moved.  There has not been any movement

17          in the scientific consensus of -- regarding DREs.

18   Q.     And the virus that you reference and discuss kind of

19          from 90 to 93, you've never tested that virus on the

20          version of software used in Georgia on the DREs,

21          right?

22   A.     No.  But actually, that's a good question.  It would

23          be -- so I have tested viral software on the previous

24          version and the subsequent version of the firmware

25          used in the DREs but not on the firmware version used

Case 1:18-cv-05391-SCJ    Document 401-1    Filed 06/27/20    Page 191 of 243

J. Alex Halderman , Ph.D.                           February 25, 2020

Fair Fight Action, Inc., Et Al. Vs. Raffensperger, Brad, Et Al.

Page 189

1          in Georgia because that was not available to me until

2          recently.

3    Q.    But it is available to you now?

4    A.    In the Curling matter.

5    Q.    And you have not yet made any analysis of that at

6          this point?

7    A.    It didn't occur to me until you asked the question

8          that that would be possible to do.

9    Q.    And how did you obtain access to that version of the

10         software in the Curling matter?

11   A.    It is in the -- it's contained in the FBI image from

12         Kennesaw State University Center For Election

13         Systems.  At least I believe that's correct.  I -- I

14         may be mistaken about that, but I do believe that the

15         firmware is there.  If my recollection is correct --

16   Q.    Got it.

17   A.    -- that analysis is not complete.

18   Q.    In paragraph 95 you reference the GEMS and

19         vulnerabilities in GEMS and BallotStation.  And I

20         know we talked about the election management servers

21         before.  But you've looked at the GEMS databases for

22         Georgia and have not found any infiltration or any

23         sort of manipulation of those databases, right?

24   A.    Yes.  The data -- the databases themselves is

25         distinct from the full contents of the server

Page 190

1        computers, which are -- which would be the -- the

2        more complete way to -- a more reliable way to look

3        for an infiltration.

4    Q.  And in 99 you say, in your opinion, an attacker who

5        infiltrated the SOS GEMS system could have spread

6        malware to the county GEMS servers be infecting the

7        CDs used to distribute the files.  And you have not

8        in your review of those CDs or any of the GEMS

9        databases found where that has occurred, right?

10   A.  I haven't had -- I don't have access to the CDs that

11       were distributed, only to the GEMS databases.  So I

12       can't assess whether the CDs actually did contain

13       malware, just that that is a viable threat factor.

14   Q.  And at the end of paragraph 100 when you say that

15       Georgia's election security countermeasures were

16       inadequate to doing these various things, the last

17       one is altering election outcomes.  It's not your

18       testimony that Georgia election outcomes have been

19       altered, is it?

20   A.  It's my testimony that we don't know and that the

21       election system did not generate adequate evidence,

22       at least any evidence that has been reviewed to date

23       to conclude that past election results were, in fact,

24       accurate.

25   Q.  Is it your testimony that we should doubt the results

Page 191

1          of the November 2018 election in Georgia?

2     A.   I wouldn't go that far.  I don't want to -- I don't

3          want to go that far.  But I do think that there is --

4          I think all of the ingredients were there for an

5          attacker to access the voting machines in polling

6          places and change the results.  The question is did

7          anyone actually do that or not.  And we wouldn't be

8          able to tell the difference from the evidence that is

9          outwardly visible one way or the other.  That's an

10         unfortunate consequence of the way the election

11         system was designed and operated.

12    Q.   So then why not doubt the November 2018 election

13         results.

14    A.   Because the election has been decided and history has

15         moved on.

16    Q.   So in your opinion, there's no value to go back and

17         try to do forensic analyses and dig up whether we

18         should rely on those results or not?

19    A.   Actually, I think that is very valuable because that

20         will teach us more about how Georgia needs to secure

21         the 2020 election.

22    Q.   How would it help with that question if it's

23         analyzing a system that's never going to be used

24         again?

25    A.   Because not all components of the system are being

J.  Alex Halderman , Ph.D.                    February 25, 2020
Fair Fight Action, Inc., Et Al. Vs. Raffensperger, Brad, Et Al.

Page 192

1        replaced.

2    Q.   Which components of the system are not being

3        replaced?

4    A.   The eNet system, the general network infrastructure

5        and computing infrastructure at the Secretary of

6        State, other infrastructure at the county level that

7        is used by election administrators.

8    Q.   So if history needs to move on and the election has

9        been decided, why not just do forensic analyses of

10       eNet, the network infrastructure of the Secretary of

11       State, the network infrastructure of county offices?

12   A.   That's going to be a less reliable way and much more

13       complicated way of trying to answer some of the

14       similar questions.

15   Q.   And you referenced the design of Georgia's election

16       system.  You're not testifying that anyone

17       intentionally designed a system that would be

18       vulnerable to hacking, are you?

19   A.   Intentionally designed, no.  Negligently maintained?

20       In my opinion, yes.

21               MR. TYSON:  Off the record for just a

22           minute.

23               (Recess taken.)

24               MR. TYSON:  All right.  Back on.

25

J.  Alex Halderman , Ph.D.                     February 25, 2020
Fair Fight Action, Inc., Et Al. Vs. Raffensperger, Brad, Et Al.

Page 193

```
 1   BY MR. TYSON:

 2   Q.    Dr. Halderman, thank you for your time today.   I

 3         don't have any further questions.

 4   A.    Thank you.

 5                  MR. HERMAN:   All right.

 6                  (Deposition concluded at 3:37 p.m.)

 7                          *   *   *

 8

 9

10

11

12

13

14

15

16

17

18

19

20

21

22

23

24

25
```

Page 194

1                  CERTIFICATE OF NOTARY PUBLIC

2        STATE OF MICHIGAN )

3                          )

4        COUNTY OF LENAWEE )

5            I, Trisha Cameron, Certified Shorthand Reporter

6        and Notary Public in and for the State of Michigan, do

7        hereby certify that the witness whose attached

8        deposition was taken before me in the above cause was

9        first duly sworn or affirmed to testify to the truth,

10       the whole truth, and nothing but the truth; that the

11       testimony contained herein was by me reduced to writing

12       in the presence of the witness by means of Stenography;

13       afterwards transcribed by means of computer-aided

14       transcription; and that the deposition is a true and

15       complete transcript of the testimony given by the

16       witness to the best of my ability.  I further certify I

17       am not connected by blood or marriage with any of the

18       parties, their attorneys or agents; that I am not an

19       employee of either of them; and that I am not

20       interested directly, indirectly, or financially in the

21       matter of controversy.

22

23

24                  Trisha Cameron, RDR, RMR, CRR, RPR, CSR

                    Notary Public, Lenawee County, Michigan

25                  My Commission Expires 5-24-24

J.  Alex Halderman , Ph.D.
February 25, 2020
Fair Fight Action, Inc., Et Al. Vs. Raffensperger, Brad, Et Al.

[& - 82]

Page 1

**&**

**&**   2:3

**0**

**05391**   1:7

**1**

**1**   4:3 9:20,23 97:18
**10**   4:4,5 5:1 55:2,3
**100**   190:14
**11**   5:5 45:2,5 56:22 57:2
**11:45**   25:25
**12**   5:8 46:12 60:8 60:9
**13**   5:11 11:4 54:15 69:7,8
**14**   5:12 97:6,7 100:12,18
**15**   5:15 102:1 182:22,23 187:13
**16**   102:3 103:18,25
**1600**   2:12
**16th**   2:4
**17**   105:14
**18**   30:16,16 105:23 107:18
**182**   5:15
**19**   107:25 165:1
**1994**   61:14
**1:18**   1:7
**1:45**   25:13 26:1

**2**

**2**   4:4 10:6,7,22 14:20,23 37:19 54:11,12 70:11 76:17
**20**   58:1,5 76:25 77:1,5 79:19,23 101:18 109:15

**200**   2:12
**2000**   18:3
**20006**   2:5
**2002**   95:18
**2006**   187:23
**2007**   92:16 147:20
**2009**   18:12
**2011**   24:12
**2014**   62:1
**2015**   97:11
**2016**   40:12 41:10 41:19 42:9 45:23 46:18 56:19 57:13 58:8 62:24 63:4 65:23 67:18,22 68:1,7,10 120:10 134:22 171:1
**2017**   37:8 41:24 42:1,18,23 48:2
**2018**   5:4 46:15 49:8 67:6 120:10 158:17 160:24 191:1,12
**2019**   4:13 9:8,9 25:7 29:21 30:9 42:23 66:24 95:18 187:22
**202**   2:6
**2020**   1:21 6:2 30:10 50:21 51:2 51:9 131:17 140:6 191:21
**2021**   50:15 123:22
**21**   111:20
**22**   113:22 114:4
**23**   77:1 114:21 117:2 120:5 121:24,25 122:16 123:12 125:1,5,11 125:16 126:10 127:21,25 129:16

**24**   132:2,12
**25**   1:21 4:6 6:2 70:11 132:18 133:3 134:3
**254**   143:3,11,24 144:9
**26**   135:5
**27**   4:7 136:5,12
**28**   179:13
**29**   4:9 139:8,14,25

**3**

**3**   4:5 10:16,19 25:10 34:21 35:23 44:3 100:12
**30**   141:5
**30339**   2:13
**31**   142:25
**31500**   1:18
**32**   144:17,19
**33**   146:8 194:23
**336-7249**   2:14
**34**   146:21
**35**   147:4 148:14 158:13
**37**   4:14 150:3
**38**   151:1 152:3
**39**   152:14
**3:37**   193:6

**4**

**4**   4:6 25:3,6 36:6 58:14 105:15
**40**   153:18
**41**   158:9
**42**   158:9 159:1
**43**   4:18 160:19
**44**   163:2
**45**   163:18
**46**   164:12
**47**   164:25

**475,000**   138:5

**5**

**5**   4:7 27:12,13 39:11,12,12,19 41:11 67:1 70:4
**5-24-24**   194:25
**50**   30:25 46:15 169:2
**51**   169:11 170:19
**52**   4:20 172:9
**54**   172:17
**55**   5:1
**56**   5:5 173:10
**57**   54:15
**59**   46:23,24 47:10

**6**

**6**   3:5 4:9 29:24 30:2 41:22 77:3
**60**   5:8 174:12
**61**   51:12 175:1
**62**   175:9
**626-5869**   2:6
**65**   177:19
**67**   178:7
**678**   2:14
**69**   5:11

**7**

**7**   4:14 37:13,15 77:3 98:3 112:24
**72**   180:1
**750**   11:6,20,25

**8**

**8**   4:18 43:20,21
**8,033,463**   5:11
**80**   58:3 116:5
**80/20**   58:7
**81**   181:10
**82**   54:14 182:14

**[87 - advocate]**    Page 2

**87** 185:24
**88** 187:10,14,24

**9**

**9** 4:3,20 52:7,9
  62:20
**90** 115:24 116:3
  156:19 188:19
**900** 2:4
**93** 188:19
**95** 189:18
**97** 5:12
**99** 190:4
**9:27** 1:20 6:3

**a**

**a.m.** 1:20 6:3
**abandon** 53:11
**abandoning** 53:16
**ability** 26:23 32:3
  32:6,10 41:6
  105:11 194:16
**able** 22:5,7 26:17
  45:17 53:19 56:17
  63:3 65:20 79:18
  87:23 100:4
  135:19 145:19
  157:1 191:8
**absentee** 105:15
  105:16,19,22
  120:16,18,23
**absolute** 87:12
  144:15
**absolutely** 111:23
  114:8 116:14
  132:25
**academic** 18:22
**academies** 34:24
  35:4 180:13
**academy** 35:1,11
  180:6 181:3 188:9

**accept** 97:22
**acceptable** 6:17,18
  92:13 93:1,2,6,12
  93:25 94:5,12
  155:4,24 156:1,21
  157:4,18 166:2
  167:4 168:22
**access** 23:17 44:9
  44:10 120:23
  134:2 149:4,11
  151:1,4,6,8,9,11
  151:15,19,20,21
  151:25 152:2,5,6,8
  152:9 161:2,5,16
  163:16 165:20
  170:13 173:7
  189:9 190:10
  191:5
**accessed** 31:11
  32:14,15,16,20,22
  161:18 169:14
**accessibility** 26:9
  26:11,19
**accessible** 33:20
**accessing** 46:21
**accompanied**
  183:11
**account** 66:16
  107:9
**accounts** 73:2
**accuracy** 177:1,2
  177:5
**accurate** 190:24
**accurately** 36:24
  136:20
**accuvote** 66:22
  67:10
**achieve** 15:6 72:7
  84:16 85:17,18,20
  100:1 109:11
  114:23

**achieves** 98:20
**achieving** 84:14
  93:12 145:5
**acknowledged**
  42:19
**acknowledging**
  44:14
**acquire** 44:15
**act** 64:13
**action** 1:5 162:24
  186:13
**actions** 185:25
  186:4
**actively** 27:8
**activist** 181:16,20
**activities** 44:11
  45:22,25 46:7,18
  51:25
**activity** 96:25
**actors** 134:18
**actual** 70:5,7
  94:24,25 95:15,17
  95:21 123:7
  131:21 177:10
**add** 152:3
**added** 95:1
**addition** 54:22
  99:9 185:5
**additional** 16:17
  51:16 59:6 66:2
  83:2 99:1,2
  165:12 168:17
  172:2 185:16
**address** 14:20
  150:19 159:4
**addressing** 111:4
**adequate** 108:15
  108:18,22 185:12
  188:8 190:21
**adequately** 140:18
  155:16 170:15

**administer** 75:13
  87:14
**administerability**
  74:10
**administering**
  74:8,18 91:18
**administration**
  28:8,9,10,12,13,15
  28:20 91:14 176:6
**administrative**
  71:19 74:21
  102:10
**administrators**
  192:7
**adopt** 64:14
  153:23
**adopted** 165:2,7
  165:14,22 166:25
**adopting** 53:18
**adoption** 49:13
  64:18 167:5
**advanced** 27:2
**advancement**
  27:23
**advantages** 84:5
**adversarial** 114:4
  114:7
**adversaries** 77:12
  77:13 78:9 81:5
  88:4 111:21
  136:14,17 176:4
**adversary** 114:25
  116:13 175:19,21
  175:22
**advertising** 24:9
**advisors** 96:12
**advocacy** 59:8
  63:14
**advocate** 34:13
  38:11 41:25 63:16
  140:18

**[advocates - asked]**    Page 3

| | | | |
|---|---|---|---|
| **advocates** 96:18 | **alleging** 14:1,12 | 186:19 189:5,17 | **applies** 184:2 |
| **advocating** 34:13 | 15:9,12 | **analytic** 17:6 | **apply** 47:18 79:14 |
| 56:2 59:21,24 | **allow** 41:20 | **analyze** 15:4 | 84:14 98:22 |
| 138:22 | 104:11 113:15 | **analyzed** 41:19 | 120:16 181:6 |
| **affect** 50:6,8 105:2 | 143:21 178:9,22 | 143:18 | **applying** 92:7 |
| 105:3,9,10,11 | **allowed** 6:13 | **analyzing** 14:21 | **approach** 17:6 |
| **affiliated** 4:8 | 62:25 161:2,5,20 | 191:23 | 53:3 99:14 |
| 27:15,16,18 28:1 | 167:9 | **andrew** 2:2 9:12 | **approached** 53:2 |
| **affirmed** 194:9 | **allows** 162:1 | **android** 143:11 | 53:4 |
| **africa** 61:15 | **alter** 14:6 103:13 | 144:1,4 | **approaches** 72:7 |
| **aftermath** 57:13 | 123:12 126:3,7 | **annual** 21:12,18 | **approaching** |
| **age** 118:22 | 127:3 151:12 | **answer** 7:11,17 | 79:11 |
| **agenda** 55:11 | 163:18 | 48:15 55:9 74:15 | **appropriate** |
| **agent** 171:7 | **altered** 61:7,9 | 109:3 157:2,4 | 155:19 |
| **agents** 112:25 | 163:23 190:19 | 192:13 | **appropriations** |
| 194:18 | **altering** 190:17 | **antivirus** 149:15 | 4:11 29:20 |
| **ago** 12:16 30:6,13 | **alternative** 84:14 | 149:16,19,20,22 | **approve** 105:4 |
| 30:22 158:5 | 84:24 141:4 | 149:25 150:5,9,17 | **approximately** |
| **agree** 36:1 37:25 | **alternatives** 20:18 | 150:20,23 169:21 | 12:1,16 102:11 |
| 44:9 45:21,25 | 20:19 74:23 141:3 | 169:23,25 170:11 | **arbitrary** 11:19 |
| 46:1 47:7 61:2 | **alumnus** 5:8 60:11 | 175:1,4 | 50:24 |
| 63:15 72:9 78:7 | 67:20 | **antiviruses** 150:16 | **architecture** 67:15 |
| 78:13,18,23 79:7 | **amended** 13:8 | **anybody** 9:10,14 | **area** 17:16 18:9 |
| 86:3 87:7 98:5 | **america** 52:12 | 123:9 | 19:5 24:19 27:5 |
| 112:7 129:20 | 72:10 | **anyway** 127:16 | 29:14 53:7 94:4 |
| 136:23 137:2 | **american** 31:19 | **apologies** 26:2 | 157:6,7,8,14,16 |
| 152:7 168:1 | **amount** 11:17 | 70:9 | 185:14 |
| 181:16,19 185:14 | 12:9 110:6 148:6 | **apologize** 96:8 | **areas** 19:24 28:14 |
| **agreed** 155:6 | **amounts** 29:5 | 156:11 | 28:24 41:18 |
| **ahead** 10:2 37:1 | **analogous** 45:14 | **app** 73:3 90:21 | **arnold** 67:4 |
| 100:10,11 174:20 | **analyses** 119:14 | **apparent** 90:6 | **arrive** 87:19 89:3 |
| 179:25 181:10 | 160:16,17 163:6 | **apparently** 41:9 | **arrived** 17:9,11,15 |
| **aherman** 2:7 | 191:17 192:9 | 60:11 62:5 | **arriving** 18:13 |
| **aided** 194:13 | **analysis** 14:24 | **appear** 23:16 | **article** 5:1,5,8 |
| **aim** 41:6 64:6 | 63:3 92:22 108:7 | **appearances** 2:1 | 56:18,20,24 57:2 |
| **aiming** 114:15 | 108:9,14,25 | **appeared** 25:17,18 | 57:11 66:16 |
| **al** 1:5,11 | 118:17 122:23 | **appearing** 2:8,16 | 170:17,21 |
| **alex** 1:17 3:4 6:5 | 144:19,24 152:4 | **appears** 25:6 30:5 | **aside** 74:5 186:9 |
| 6:10 25:24 60:24 | 156:22 166:10 | **application** 21:6 | 187:13 |
| **aligned** 169:19 | 167:6,10,18 | **applications** 38:8 | **asked** 7:17 13:1 |
| 171:14 | 168:13 186:16,16 | 103:23 138:25 | 74:14 100:18 |

Case 1:18-cv-05391-SCJ    Document 401-1    Filed 06/27/20    Page 200 of 243
J. Alex Halderman , Ph.D.    February 25, 2020
Fair Fight Action, Inc., Et Al. Vs. Raffensperger, Brad, Et Al.

[asked - audits]    Page 4

146:4 166:24 189:7
**asking** 7:21,22 13:18 51:6 130:10 187:3
**aspects** 28:13
**assembly** 64:25
**asserts** 159:12
**assess** 93:8 99:10 190:12
**assessed** 164:3 179:18
**assessing** 79:25 81:10,14 92:11 94:12
**assessment** 20:4,6 46:15 59:25 61:2 107:2,10 149:2 158:4,11,12,18,19 160:3,12 168:19 181:18
**assessments** 112:1 118:24,25 119:2 158:24 159:24
**assist** 68:6
**assistance** 180:8
**assistant** 18:17
**assisted** 67:24 69:25
**associated** 102:9 103:23
**assume** 76:12 166:24
**assumed** 109:7
**assuming** 9:23 18:3 21:1,22 24:4 24:21 36:18 54:16 60:16 75:4 98:23 108:6,13,17,25 111:24 121:12 128:4 129:21

131:2 149:9 158:7 173:12
**assumptions** 13:6 109:2
**assurance** 27:3
**atari** 139:22
**atlanta** 1:3 2:13
**attached** 5:20 17:2 19:15 194:7
**attachment** 54:12
**attack** 14:25 15:3 23:19 39:16,21 40:6,9,25 46:11 50:9 80:3 81:4 82:7 84:19 87:8 87:10,12 89:8 93:11 109:17 114:18,24 115:12 115:20 116:1,12 116:25 117:1 120:4,4,25 121:23 123:12 125:1,8,11 125:16 127:19,22 127:25 128:3,12 128:17 129:16,19 129:23 140:14 145:20 162:6,10 162:12 163:18 173:25 175:7 180:16 187:2
**attacked** 135:10 137:3,9
**attacker** 14:6 15:6 23:10,15 110:6,14 122:9 126:20,23 127:13 134:1 143:9,20 151:10 153:9 161:2,5 162:3 163:23 166:18 174:13 190:4 191:5

**attackers** 32:19 62:2 78:18,23 117:3,13 120:25 135:21 139:24 143:21 149:8 157:1 161:21 169:2 170:8 176:2
**attacking** 5:3 113:1
**attacks** 23:22 30:24 31:3 40:13 52:24 71:22,24,25 73:13 74:24 77:16 79:7 80:24 81:6 81:13 83:14,16 88:12 93:10,14 105:2,2,8,9,10 106:10,15,16,18 106:20,22 109:23 110:3 115:7 119:24 121:25 128:6,23 130:19 131:20,25 154:21 176:8 177:6 179:11 183:23 184:7 187:25
**attempt** 20:18 39:22 77:13 127:19 166:18 171:7
**attempted** 23:16 61:19 62:3
**attempting** 112:5
**attempts** 46:8 160:19 177:13
**attend** 37:8
**attention** 53:6,8 53:10 54:3 152:16 152:18,19
**attorney** 9:14

**attorneys** 9:13,17 12:15 194:18
**attracted** 18:7
**attributed** 57:12
**attributes** 26:12 26:14
**audit** 34:14 36:7 49:9,10,15,24,25 50:4,7,14,18,21,23 50:24 51:2,9 74:17 75:19,20 115:6 123:15,20 123:21 124:4,12 124:22,25 125:15 125:18,19 127:21 128:5 129:1 130:2 130:5,9 140:15 173:14,15 179:9 179:11
**audited** 74:7 125:12 136:22 139:7
**auditing** 29:16 69:14 70:1 71:4 80:15 110:10,13 110:17 123:25 124:2 154:16
**auditmark** 172:12 172:13 173:21,21
**audits** 34:22 36:20 38:11,24 39:1,9 49:6,13,21 50:11 70:20,25 71:11 75:18 78:12 115:13,19 124:6,8 124:16,18,21,21 128:8 130:15 153:12 155:13 173:13,23,24 174:1 179:21,22

**[august - believe]**                                      Page 5

**[believe - cameron]**                                    Page 6

| | | | |
|---|---|---|---|
| 25:18 35:15 47:23 | **bill** 12:4,10 64:13 | **boards** 112:14 | **btyson** 2:15 |
| 48:10 50:16 54:20 | **billion** 23:12 | **bolstered** 46:15 | **build** 119:21 |
| 56:13 57:22 58:7 | **billions** 89:19 | **bono** 11:25 68:12 | **built** 98:14 |
| 64:20 73:9 74:6 | **biographical** 10:4 | **book** 163:3 | **bullet** 41:25 45:9 |
| 74:16 75:4 84:3 | **bipartisan** 32:1 | **books** 101:16 | 47:3,8,25 48:5,11 |
| 85:21 90:7 91:17 | 64:11 | 104:6 163:1 | 48:13,21 49:6 |
| 91:17 94:22 96:1 | **bishop** 25:23 | **bottom** 35:23 36:6 | 51:13 |
| 97:11,25 102:1 | **bit** 12:11 16:24 | 58:14 77:3 92:15 | **bunch** 95:1 |
| 113:23 116:11 | 17:8 22:7 26:4,25 | 92:24 105:14 | **business** 20:24 |
| 117:17 124:21 | 28:4 49:7 65:10 | 107:18 147:20 | 21:1 |
| 133:13 135:2 | 76:10,12,15 | 179:13 187:24 | |

|  **c**  |
|---|

| | | | |
|---|---|---|---|
| 146:25 152:18 | 105:14 132:18 | **box** 51:23 | **c** 21:9 122:16 |
| 159:19 161:12 | 133:7 184:21 | **boy** 16:14 | 123:12 125:1 |
| 163:13 173:23 | **black** 171:8 | **brad** 1:8 6:11 | 128:7,23 129:7 |
| 177:22 182:2 | **blindly** 38:8 | **break** 7:18 33:4,5 | 130:1 138:16,16 |
| 189:13,14 | **blood** 194:17 | 37:1 132:21,22 | 138:18,18,20,21 |
| **bell** 16:20 | **blow** 31:18 | 174:19,20 175:23 | 139:3,3 |
| **benaloh** 25:23 | **bmd** 83:9 85:15 | **breakdown** 64:24 | **cable** 66:7 |
| **benedict** 67:4 | 86:25 93:23 | 93:21 | **california** 8:22,23 |
| **benefit** 24:7,8 99:1 | 105:22 107:20 | **breaks** 7:15 | 92:15,24 118:15 |
| 124:19 | 129:5 137:18,20 | **brennan** 27:23 | 119:1 136:8 |
| **benefits** 98:20 | 144:12,14 150:14 | **brian** 6:23 | 139:14 146:22 |
| 99:3 109:25 | 154:21 156:1,5,21 | **bridge** 17:25 | 147:1,19,25 148:5 |
| **bernard** 182:25 | 167:17,20 168:10 | **bridged** 17:21 | 148:21 150:13,20 |
| 183:2 | 175:4 180:15,21 | **briefings** 42:23,24 | 152:11 153:18,24 |
| **best** 7:6,10,12 19:4 | 181:1,6 186:1 | 42:25 43:4 | 154:3,7,15,18,18 |
| 28:16 34:14,22 | **bmds** 77:14,15 | **briefly** 96:15 | 154:22,23 155:1,2 |
| 42:12 56:13 74:7 | 78:24 79:2 105:16 | **briefs** 13:14,17 | 155:7 164:21,25 |
| 74:17 75:5,12 | 105:20 135:23 | **bring** 53:6,8 75:24 | 165:23 166:13,21 |
| 76:6 91:17 113:16 | 150:15 151:7 | **bringing** 53:10 | 166:25 167:23 |
| 116:20 145:1,5 | 153:12,15 154:19 | **brings** 73:10 | 168:11,21 |
| 183:25 184:5 | 154:24 155:3,8,8 | **brittleness** 118:22 | **california's** 147:5 |
| 194:16 | 155:11,12,14,17 | **broad** 64:11 | 149:12,14 150:7,7 |
| **better** 7:14 34:1 | 157:17,20,21 | 134:19 188:7 | 153:8 154:11 |
| 102:20 174:15 | 165:6,20 168:17 | **broader** 19:5 | **call** 177:1 |
| **beyond** 8:19 12:20 | 173:12 178:10,22 | 20:13 99:3,5,21 | **called** 21:9 23:3 |
| 13:1,4 15:18 | 179:2 180:17,24 | 103:3 | 26:10 35:4 99:24 |
| 16:12 46:2,5 | **board** 63:24 96:12 | **broadly** 13:21 | 119:16,18 180:12 |
| 51:10 81:2 83:25 | 121:9 124:5,7 | 19:14 28:12 71:12 | **cameron** 1:22 |
| 93:23 126:15 | 178:11 184:19 | **bryan** 2:10 | 194:5,24 |

Case 1:18-cv-05391-SCJ Document 401-1 Filed 06/27/20 Page 203 of 243

J. Alex Halderman , Ph.D.
February 25, 2020
Fair Fight Action, Inc., Et Al. Vs. Raffensperger, Brad, Et Al.

**[campaign - chose]**

**campaign** 57:7
68:3,4,5,13,16,19
68:22,23 69:2
**campaigns** 68:18
**candidate** 69:1
122:11 182:15,19
182:20
**candidates** 14:7
182:20 183:12
**capabilities** 32:19
44:15 114:12
116:24 163:9
**capability** 47:7
**capable** 175:19
**capacity** 1:9
**capital** 43:1
**card** 107:19 168:9
**cards** 108:1,24,24
109:8 165:6,18,21
**career** 18:22 60:24
**careful** 128:5
137:6
**carefully** 44:13
126:11 128:1,8
130:14 164:19
**carolina** 27:22
**carpathian** 111:25
**carries** 99:2
**case** 1:7 9:7 10:10
11:7,19 12:4,14
13:6,8,11,14,20,21
13:25 36:24 91:16
93:19 95:24 98:20
100:16,22,24
127:16 148:18
158:8 159:11,17
162:19,24 164:18
166:16 178:5,15
178:23
**cases** 11:11 44:25
130:23,23 150:10

154:20
**cast** 70:16 105:11
**casting** 119:25
**catch** 180:15
**catching** 156:3
**categories** 83:14
83:15 177:16
179:22
**categorize** 110:13
139:17
**categorizing** 87:18
**category** 109:22
**caucus** 72:25
**caucuses** 72:20
**cause** 27:22 87:24
119:24 122:11
162:4 164:2
184:24 194:8
**caused** 40:8,17,19
86:18 128:19
**causes** 17:6 20:13
**causing** 20:16
39:14 90:17
**caveat** 111:1
**cd** 106:5
**cds** 190:7,8,10,12
**cellphone** 90:7,16
90:21
**cellphones** 90:9,20
**censys** 21:9,14,22
22:4 24:4,9
**center** 27:23
189:12
**central** 29:11
101:2,10 138:9
**certain** 26:21
36:15 41:4 53:23
55:20 71:22 72:7
74:22 83:14,15
94:8 105:10 178:3
179:10 186:1,5

**certainly** 14:5,16
18:10 27:8 31:15
31:15 47:21 59:24
63:18 64:10 70:23
102:18 117:23
118:10 132:22
144:8 166:1
177:12
**certainty** 40:18
181:6
**certificate** 23:3,12
23:16,21 194:1
**certificates** 23:13
**certification** 50:1
50:1 142:5,18
146:13,18,20
150:22,23 154:4
157:10 171:2
**certifications** 8:23
**certified** 48:7
141:25 142:1,3,4,7
146:8,10 165:1,9
170:25 180:7,7
194:5
**certify** 153:19
154:12 194:7,16
**chain** 28:16 48:22
108:15,18,22
109:9,12 169:1
171:25 184:21
**chains** 172:1
**challenges** 71:10
75:25
**challenging** 18:10
99:12
**chance** 7:2 58:1,3
58:5 183:23
**change** 35:16 42:8
53:1 72:12 76:10
82:15 87:23
107:12 110:1

115:8 117:6
126:17 142:11
156:25 161:21
162:4 185:21
191:6
**changed** 35:12,19
35:21 44:7,18
57:15 58:2 60:25
62:15 65:22 106:2
162:14 176:24
**changes** 18:5 51:4
65:19 76:4 104:23
104:24 105:7
125:9,9 131:1
142:21,22 178:16
**changing** 50:25
83:3 119:17
**chaos** 41:10 87:12
128:20 129:25
164:2
**characterization**
45:25
**characterize** 39:1
50:7 148:8,10,11
148:13
**charge** 11:11,21
**cheap** 144:17
**cheat** 127:16
**check** 12:17 58:6
63:1 118:16 164:3
164:10,11 185:19
**checked** 51:23
**checking** 185:8
**chevalier** 2:3
**chief** 144:24 145:2
**choice** 85:23
**choose** 22:11,17
51:1
**chooses** 148:6
**chose** 31:19 148:5
153:19

**[chosen - computer]**

Page 8

| | | | |
|---|---|---|---|
| **chosen** 89:22,22 90:13,25 91:10 | **coat** 66:17 | **committee's** 43:16 47:25 | **complex** 140:1 |
| **circle** 2:12 | **code** 99:1 125:9,10 126:3,7 137:18,22 137:24 138:6,10 138:12 139:9,11 140:8 146:10 147:23 158:20 160:13 | **common** 27:22 70:20,24 141:7,8 | **complexities** 49:22 |
| **circumstance** 73:14 129:13 178:10 | | **community** 23:22 44:15 112:2 | **complexity** 22:3 137:16 139:9,16 |
| **circumstances** 11:23 58:25 74:22 84:17 151:5,10 | | **companies** 20:21 20:24 21:7,10 22:17 171:7 | **complicated** 192:13 |
| **cite** 126:12 135:7 137:10,16 143:2 178:6 181:11 182:13 188:7,8 | **collaborative** 124:15 | **company** 20:23 21:1,3,8,13 22:5 22:11,24 169:22 170:2,8,13 | **complicates** 71:13 |
| | **collected** 70:18 | | **complies** 47:24 |
| | **column** 70:4,10 | | **comply** 48:7 |
| | **columns** 70:9 | | **component** 14:1 96:21 101:1 103:2 103:12,15 |
| **cited** 9:1,3 | **combination** 128:24 | **comparative** 81:15,20 82:1,4 | **components** 28:20 29:12 31:4 43:13 75:1 78:19 79:1 81:17,21 88:5 100:25 103:20 115:15 133:4,25 134:23 135:5 136:6 142:25 150:4,17,19,22,24 161:7 162:20 169:12 191:25 192:2 |
| **civil** 6:14 | | **comparatively** 92:11 | |
| **clarification** 111:17 | **combined** 36:20 | **compare** 82:2 174:16 | |
| **clarified** 74:15 | **come** 64:16 65:13 79:13 81:9 84:2 92:18 105:13 134:1 135:15 178:14 | **compared** 103:2 118:8,9 137:17 138:1 144:2,4,5 | |
| **clarify** 68:25 74:13 | | **comparison** 145:25 148:17,22 | |
| **clean** 93:20 | | | |
| **clear** 15:4 83:17 83:18 84:21,23 85:25 87:21 168:2 | **comes** 92:6,6 94:9 103:16 | **comparisons** 174:3,5,14 | |
| | **coming** 84:12 123:14 | **compartmentalize** 100:4 | **compromise** 62:3 94:24 95:3,4,5 113:7 116:18 122:1,2,7 123:4 143:22 157:2 |
| **clearer** 7:14 | | | |
| **clearly** 22:21 86:8 | **commencing** 1:20 | **compensated** 11:6 | |
| **clinton** 57:7 66:9 68:4 | **commercial** 98:4,9 98:13 138:24 | **compensation** 24:3 | |
| | **commission** 127:12 180:8 194:25 | **competing** 88:24 | **compromised** 95:10,13,25 113:12,15,18,20 188:2 |
| **close** 36:22 79:23 109:23 126:18,21 126:24 127:14,17 127:18,20 157:1 180:17 183:23 184:7,25 187:6 | | **complaint** 13:8 | |
| | | **complete** 10:18 49:10 142:23 189:17 190:2 194:15 | |
| | **commissioned** 92:16 158:25 | | **compromises** 55:24 |
| **closed** 99:12 100:2 100:2 | **committee** 4:16,19 30:4,23 31:6 32:2 32:9 37:7,9,11,16 40:21 43:24 44:6 44:9 45:3 47:2 48:1,3 63:23 113:10 134:20 | **completed** 58:13 | **computer** 17:6,13 19:3,13 23:9 37:24 38:1,4 61:18 81:6 87:13 96:24 103:17 135:8 136:16,24 |
| **closely** 112:1 169:19 | | **completely** 107:24 118:25 | |
| **closeness** 156:8 | | | |
| **closer** 33:1 | | | |

**[computer - correct]**                                              Page 9

137:1,2,5,14
139:19 140:9
144:22 151:14,15
151:17,23 152:22
170:17,21 174:9
194:13
**computerized**
140:17
**computers**  37:21
38:9 80:4,8 180:2
190:1
**computing**  19:4
22:2 139:16,17,21
139:22 192:5
**conceal**  174:13
**concept**  61:1
67:21 112:7
156:11
**concepts**  112:8
**concern**  53:21
64:8 87:1
**concerned**  106:15
106:16,19 109:17
115:8
**concerns**  28:10,18
86:22
**conclude**  31:15
42:20 85:7 126:23
129:3 159:14
190:23
**concluded**  30:23
32:9 54:16 193:6
**concludes**  185:13
**concluding**  88:7
**conclusion**  42:16
80:25 85:9 107:17
113:16 118:3
134:19 150:11
164:6
**conclusions**  89:3
100:14 107:6,15

108:19 109:1
135:17 176:20
**conclusively**  40:13
**condition**  155:7
**conditionally**
164:25 165:9
**conditions**  153:22
153:24 154:4
155:4 165:12
166:4,6,7,13 167:1
167:5 184:5
**conduct**  20:3,5
51:1 65:18 130:18
**conducted**  35:8
42:10 49:9 50:17
65:16,19 101:21
119:1 167:10,13
**conference**  25:8
**conferences**  24:22
**confidence**  65:14
88:22 160:10,15
160:15
**configuration**
161:16
**confirm**  69:17
75:14 180:25
**conflicting**  135:17
**confusing**  7:23
**congress**  29:18
43:2 55:23 64:12
**congressional**
42:22
**connect**  23:5
**connected**  26:9,12
114:1 132:19
133:5,9,17 134:4
135:6 194:17
**connection**  23:7
160:22
**cons**  99:15,17

**consensus**  35:15
188:7,17
**consequence**
191:10
**conservative**
27:25 42:14
**consider**  28:7,11
28:21 29:11,15
38:24 106:25
176:18
**consideration**
72:11 186:15
**considerations**
36:2 87:6
**considered**  176:22
**considering**
176:17
**considers**  80:14
**consistent**  31:22
46:17 51:7,11
59:12 63:1 91:21
91:22 152:17
**consistently**  59:5
72:2
**constitutional**
71:19
**constrained**  88:13
90:1
**construct**  157:19
**consulting**  20:20
21:17,19
**consumers**  90:1
**contact**  12:12
**contacted**  12:15
12:18
**contain**  148:16
190:12
**contained**  161:24
189:11 194:11
**contains**  133:13

**contents**  189:25
**contest**  131:3,9,13
144:3
**context**  19:11
24:10 47:1 81:6
84:11 92:13 94:6
94:12 126:2
127:15 129:5
137:7 143:7
**contexts**  174:10
**continue**  58:16
163:25 164:1
178:10,22
**continues**  112:4
**contours**  8:14
**contraband**  66:18
**contracted**  159:23
**contracting**  48:14
51:17
**contractors**
171:21,22
**contrary**  72:16
**contrast**  85:16
**contributions**  25:1
**controversy**
194:21
**convenience**  89:24
90:15
**conversations**  7:7
15:20
**convince**  167:23
**cooperation**  20:10
161:4
**copy**  54:9
**core**  63:13 137:3
**corporation**  21:3
**correct**  9:9 11:7,8
14:3,13,21 15:14
16:15 18:23,24
19:19,20 24:1,5
27:4 31:11,14

[correct - database]                                          Page 10

| | | | |
|---|---|---|---|
| 32:7 34:9,15,19 35:14 36:4 38:16 39:9,10 40:9,17,25 41:7,16,17 44:22 47:16 48:1,9 50:1 50:14,22 51:2 53:7,17 54:18,24 56:15 58:11 66:25 68:10,11 69:5,6 71:9,19 74:9,11 75:6 78:3 84:1 87:5 92:22 95:1 102:7,8 106:8,17 107:2 111:9,15 112:20 114:15,16 119:8,11 123:2 124:1 125:3,4 127:24 130:2,25 132:13 136:9,10 137:7 139:5 142:2 142:8 146:14 157:17 158:5,23 162:14,15 163:3,4 163:25 167:14,22 168:5,23 170:22 173:14 174:10 177:11 181:15 183:2,9 187:16 189:13,15 **corrected**  104:9 110:19 130:8 148:25 159:19,20 **correcting**  88:12 **correction**  129:14 **correctly**  26:18 38:9 140:23 158:18 **correctness**  66:2 179:18 **cost**  160:17 164:11 | **counsel**  12:22 13:2 13:5 15:19 113:11 **count**  38:14 75:13 75:22,23 76:2 101:2,7,10 138:9 **counted**  38:12,23 53:1 61:19 75:17 **countermeasures** 190:15 **counties**  121:12,16 178:21 **counting**  75:5,8,8 75:10,15,24 76:5 113:24 **country**  19:4 **county**  16:4 50:19 105:25 107:24 108:12 112:14 127:12 135:22 155:2 178:2 179:4 190:6 192:6,11 194:4,24 **couple**  7:1 94:16 97:17 137:12 **coupled**  55:15 155:11 **course**  33:8 61:4 89:16 **courses**  19:7,8,17 **court**  1:1 7:6 16:19 **cover**  19:23 26:19 **covered**  26:6 43:13 83:24 94:22 102:1 109:15 112:18 146:25 163:2 175:1 179:24 **covers**  26:20 **create**  53:3 72:4 74:23 88:23 | 133:25 172:1 **created**  83:3 **creates**  71:1 75:2 75:10 152:12 165:19 170:5 **credibly**  99:10 **critical**  23:1 141:21 161:7 166:20 **critically**  136:18 **criticism**  134:4,6 **cross**  92:1 93:17 **crr**  1:22 194:24 **crucial**  23:6 **crucially**  33:21 **cryptographic** 100:8 **csr**  1:22 194:24 **cues**  182:10 **curiosity**  72:19 73:6 **curling**  9:6 16:11 16:13,16 158:8 159:11,17 178:14 189:4,10 **current**  12:8 68:23 97:25,25 106:7,11 123:24 155:18 178:15 **currently**  18:19 49:15 115:18 116:18 123:16 124:4 125:21 146:1 **custody**  28:16 48:22 108:15,18 108:22 109:9,12 **custom**  98:14,24 119:20 **customary**  11:9 | **cut**  87:10 **cv**  1:7 17:1 19:17 24:12 42:22 54:6 54:9,15 **cyber**  80:7,12,20 80:24 81:2,3 84:25 85:6 108:8 116:8,23 158:4 187:25 **cyberattack**  57:21 61:8 122:4,6 **cybersecurity** 17:16 19:9,10,14 19:22 28:5 51:15 51:17 82:14 83:21 83:22,25 84:5,10 84:16 85:13 87:5 89:12 96:21 98:12 114:11 119:2 146:18 159:23 160:5,9 **czech**  169:22 170:2,13 **d** **d**  2:2 125:5,7,11 125:16 128:7,23 129:7 130:4,8 **d.c.**  2:5 **damage**  20:13 **dangerous**  20:9 **daniel's**  46:15 **data**  12:22 13:3 14:14 32:4 103:9 103:16,16 104:2,3 104:6,12,14,20,24 122:2 133:20 161:3,17 163:19 163:23 189:24 **database**  102:6,9 102:15 103:14 104:21 117:6,11 |

**[database - determining]**    Page 11

117:14 119:6,18
119:22 120:7
129:18 133:9,12
133:20 158:3
160:11
**databases** 117:21
118:2,20 119:3
123:1,6 189:21,23
189:24 190:9,11
**date** 58:18 141:11
141:17 142:15
153:25 190:22
**day** 8:6 30:6 40:2
40:3,8,17 41:14
95:21 105:12
107:13 121:2
178:2
**deal** 19:18
**death** 61:23
**decade** 58:18
**decertified** 187:21
**decide** 82:18
**decided** 41:9
72:10 119:21
164:22 191:14
192:9
**decides** 140:5
**decision** 88:14,17
88:18 89:2,7,10,11
148:3,9 154:11
164:8
**decisions** 100:15
**decrease** 164:11
**decreasingly**
139:1
**dedicated** 38:5
69:21
**defend** 33:10
**defendant** 6:11
**defendants** 1:12
2:16

**defense** 71:21
78:12 92:9 175:3
**defenses** 78:21
83:7
**defensive** 80:16
**define** 49:17,19
**defined** 99:23
100:8
**definitely** 78:1,4
114:18 116:14
151:18
**definition** 162:21
**definitions** 26:13
49:20
**definitively**
177:24
**degree** 90:14 93:1
93:2,6,13,25 94:6
118:15 155:22
156:21 168:13
**degrees** 92:13 94:8
94:12 115:23
**delay** 86:18
**delightfully** 63:24
**demand** 179:1
**demillo** 15:24
181:13
**democracy** 31:19
101:12
**demonstrate**
20:14
**demonstrates**
185:18
**demonstration**
67:5,7,8,11
**demonstratively**
95:10
**department** 19:3
138:22
**depend** 106:20,22
109:4 160:16

**dependencies**
141:11,21
**depending** 129:19
**depends** 11:23
15:6 24:10 34:4
49:16,19 58:24,24
63:18 74:4 98:19
123:23 130:21
142:22 143:8,8
149:23,23
**deployment** 156:5
157:13
**deposition** 1:17
4:2,3 6:10 7:3,20
8:8,9 9:4,6,11,18
9:23 193:6 194:8
194:14
**depositions** 13:10
**derivation** 178:6
**describe** 15:2
26:25 52:16 96:15
110:23
**described** 12:20
63:2
**describing** 120:5
**description** 13:19
46:1,4 63:16
**design** 29:3,5,12
29:15 70:20,25
72:17 88:25
101:20 124:20
157:21 169:11
192:15
**designed** 75:21
80:17 87:25 98:24
135:13,19 136:11
152:13,15 172:18
185:7 191:11
192:17,19
**designing** 29:2
141:7

**despite** 77:17
**destroy** 32:3
**detail** 117:23,25
121:11 159:14
**detailed** 132:19
159:24
**details** 10:4 94:18
160:16
**detect** 5:16 50:25
75:22 127:22
129:16 130:24
131:12,12 132:10
150:9 173:25
177:25 179:10,23
**detectable** 67:16
67:17 129:23
**detected** 61:20
62:6 93:10,12
127:25 128:4,7,14
128:18 129:8
130:1,4,7,13
134:14 173:11
180:17
**detecting** 88:11
183:23 184:7,25
**detection** 129:13
130:10 150:17
**determination**
168:8
**determine** 84:8
91:24 92:2 93:16
127:2 155:25
166:11,15,17
167:20
**determined** 117:1
137:8
**determines** 86:8
**determining** 92:25
94:5 127:13
186:18

Case 1:18-cv-05391-SCJ    Document 401-1    Filed 06/27/20    Page 208 of 243
J. Alex Halderman , Ph.D.                              February 25, 2020
Fair Fight Action, Inc., Et Al. Vs. Raffensperger, Brad, Et Al.

[develop - documents]                                          Page 12

| | | | |
|---|---|---|---|
| **develop**  124:16 | **die**  20:16 | 81:19 82:11 91:20 | 132:19 151:1 |
| **developed**  46:14 | **difference**  85:13 | 163:10,13,14,24 | 155:23 |
| 169:18 | 105:1,6 106:9 | **disadvantage** | **discussions**  144:21 |
| **developing**  97:1 | 107:14 110:23 | 61:20 | **dishonest**  76:4 |
| 98:16 | 114:14 148:2 | **disadvantages** | **disparate**  14:18 |
| **development** | 191:8 | 84:6 | 15:11 |
| 124:12 141:22,23 | **differences**  58:4 | **disagree**  35:1,3 | **dispute**  136:13 |
| 145:2 146:5 169:3 | 82:6 166:20 | 47:12 74:12 | **disrupt**  20:12 |
| 171:9 | **different**  31:23 | 154:11 | **disrupted**  130:23 |
| **deviation**  66:5 | 46:11 49:20 67:9 | **disc**  142:6 | **disruption**  87:24 |
| **deviations**  57:20 | 73:13 88:19 | **discipline**  94:7 | **disruptive**  185:25 |
| **device**  33:15 34:9 | 102:19 146:22 | **disclosure**  19:25 | 186:4 |
| 34:18 36:10,16,17 | 148:10 150:20 | **disconnected** | **distinct**  112:6,8 |
| 36:18 73:20 82:16 | 153:2 157:21,22 | 135:19 | 189:25 |
| 82:22 83:1 91:1 | 166:17 172:24 | **discord**  14:6 | **distinction**  110:21 |
| 93:7 97:22 101:4 | 175:13,14 177:15 | **discounts**  11:10,13 | 112:15 129:6 |
| 138:1 145:16,18 | 177:16 | **discover**  50:9 | 148:12 |
| 146:1 149:18 | **differently**  148:13 | 157:24 | **distinguish**  91:15 |
| 153:3 172:21 | **differing**  125:6 | **discovered**  39:8 | 129:12 148:14 |
| 177:14,25 178:3 | **difficult**  64:23 | 123:4 160:23 | 177:9,16 |
| 181:12 183:19 | 98:17 138:20 | **discovering** | **distinguishes** |
| **devices**  5:18 19:15 | 151:8,24 172:7 | 139:25 | 111:13 168:11 |
| 26:8 33:18,22 | **difficulty**  110:10 | **discovery**  6:12 | **distribute**  179:8 |
| 35:2,6,10,14 37:24 | 145:4 | **discriminatory** | 190:7 |
| 42:2,7,9,11,14,17 | **dig**  67:14 94:18 | 13:23 | **distributed**  190:11 |
| 42:21 43:12 59:21 | 191:17 | **discuss**  39:13 43:5 | **district**  1:1,2 |
| 59:25 60:2 65:1 | **digital**  123:13 | 54:17 163:18 | **division**  1:3 |
| 73:17 82:11 86:4 | 127:23 172:19 | 188:18 | **docket**  13:4,13,15 |
| 91:19 93:18 98:2 | 173:16,19 | **discussed**  14:4 | **document**  9:24 |
| 101:1 136:13 | **diligence**  51:25 | 41:5 43:7 46:20 | 33:7 54:15 97:9 |
| 145:23,24 151:13 | **direct**  148:22 | 49:7 66:10 113:6 | **documentation** |
| 152:24 153:5 | **direction**  12:19 | 113:23 133:7 | 8:13,21,25 136:8 |
| 156:16 166:23 | 76:10 | 136:7,16 141:12 | 154:6,8 163:6 |
| 175:11 176:20 | **directly**  18:15 | 159:7 160:21,21 | 172:15 |
| 177:3,21 180:2 | 114:1 133:4 | 188:1,14 | **documented**  94:23 |
| 182:1 184:10 | 134:17 194:20 | **discusses**  174:3 | 95:24 101:20 |
| 185:22 188:13,16 | **disabilities**  26:22 | 177:14 | 106:12 143:2 |
| **devoid**  159:13 | 26:22 33:21 42:3 | **discussing**  65:12 | **documenting** |
| **dhs**  112:2 | **disable**  163:16 | 70:14 132:2 177:7 | 176:6 |
| **diagram**  129:11 | **disabled**  59:22 | **discussion**  34:25 | **documents**  8:16 |
| | 73:14,23 74:5 | 54:19 64:15 107:4 | 8:16,17,19 9:3 |

**[documents - election]**                                                          Page 13

12:23 13:2,3
102:2
**doing**  59:3 63:11
  67:21 72:3 147:22
  166:16 190:16
**dollars**  89:19
**domain**  69:22
**domestic**  171:21
**domestically**
  169:18 172:3,4
**dominican**  68:24
**dominion**  8:10,17
  8:21,24 12:25
  13:1 86:9 100:21
  101:20,24 102:3
  106:4 122:5 126:3
  126:5,8 135:25
  136:2,4,6,12
  137:22 139:9
  140:7 141:24
  144:25 145:6,12
  146:4 147:2 149:3
  149:9 150:4
  152:15,23 153:10
  153:14,19 154:5,9
  154:12 155:15
  163:5 169:4
  170:20 171:16
  172:14,23,25
**dominion's**  137:17
  145:9 153:1
  172:15 173:2
  174:15
**door**  45:20 46:10
**doorknob**  45:17
**doubt**  111:21,23
  112:17 114:9
  159:21 173:5
  190:25 191:12
**downsides**  106:6

**downstream**
  141:21
**dr**  4:9,14 6:10,21
  11:4 15:24,25
  25:5 37:6 45:3,9
  45:11 60:7 96:7
  174:25 181:13
  193:2
**drastic**  186:13
**draw**  112:6,15
**dre**  37:20 56:14
  66:22 73:20 110:7
  110:20 111:14,16
  111:18,18 187:16
  187:24
**dres**  36:19 38:22
  43:5 109:20
  110:15 180:5,7
  187:11,18 188:2,6
  188:8,17,20,25
**dubbed**  66:7
**due**  58:2,4 89:21
  134:12
**duly**  6:6 194:9
**duma**  2:11
**dynamics**  55:16
  55:17

---

**e**

**e**  21:9 37:11 125:7
  126:10 127:21,25
  128:7,24 129:7
  130:7,13 131:20
  163:3
**eac**  48:7 141:25
  142:1,3,5,12
  146:11,17,20
  150:21,23 171:1,2
  180:7
**eac's**  146:13
**earlier**  16:11,12
  38:3 53:22 63:2

83:24 84:8 88:2
  91:17 112:18
  113:6,23 141:12
  155:23 169:22
**easier**  5:10 60:21
  71:17 72:17 99:10
  99:25 143:20
  157:23 187:2
**easy**  7:8 10:4 28:4
  164:5
**edges**  107:13
**editorial**  54:23
  55:6
**educate**  43:1
**effect**  14:5,8,24
  20:15
**effective**  56:1
  67:10 184:16
**effectively**  109:11
**effects**  13:24
**efficiently**  69:14
**effort**  41:12 48:21
  59:7,8 65:17
  124:15 147:22
  148:3
**efforts**  30:14
  43:17 67:24 68:12
  77:17
**eight**  159:6
**either**  35:13 36:24
  48:7 84:18 87:1
  103:12 108:7,25
  162:10 194:19
**elaborate**  20:7
**election**  4:21 5:6
  13:21 14:7 15:22
  16:4 18:3 19:9,11
  24:13,16,17,18,18
  25:2 27:3 28:8,9,9
  28:12,13,14,20
  29:2,3,6 30:14

31:4 33:10 38:15
  38:20 39:5,20,22
  40:2,3,8,17 41:13
  41:14,18 43:6,14
  43:18 44:19,22
  45:23 46:18 49:9
  49:10 50:22 51:4
  52:11,23 53:13,15
  54:17,24 57:14,15
  57:20,24 58:3,8,11
  61:14,21 62:1,4,8
  62:15,24 63:4,20
  64:8 65:1,15,23
  66:3,8 67:4,22
  70:21 71:13 72:2
  72:18 73:11,12
  74:24 75:25 76:3
  77:7,14 78:7,10,13
  78:19,25 79:12,15
  80:5,8,18 81:1,16
  83:8 84:1 85:8
  86:11,14,16,17,19
  86:22,24 87:8,14
  87:23 88:2,4,5,9
  88:25 89:8,12
  90:4,18 91:1,14
  92:13,18 93:1,25
  94:6,12,24,25 95:6
  95:16,20,21,22
  96:18,20 100:19
  101:13 104:1,2,5
  105:12,25 106:25
  107:7,18,21 108:1
  108:6 109:7,19
  112:5,6,11,20
  113:24 115:9
  116:8,15 117:4
  121:2,9,14 122:19
  123:13 124:5,7
  126:22 130:22
  131:3,9,13,13,18

**[election - evidence]**                                    Page 14

131:21,23 132:4,5
132:8,15 133:17
135:24 140:24
144:3 155:20
156:8,24 157:1
160:24 163:24
167:22 168:5
170:10 171:10
173:11 175:14
178:11 179:4,9
180:3,4,5,8,10,17
180:18 181:19
182:15,16 183:23
184:19 185:24
186:3,7,7 187:5,7
187:9 189:12,20
190:15,17,18,21
190:23 191:1,10
191:12,14,21
192:7,8,15
**elections**   5:4 16:3
24:20 28:6,10
29:16 36:23 41:23
43:3 51:20 53:8
54:1 56:19 58:22
61:1,3,4,7 64:13
64:15 69:14 74:8
74:18 75:13 86:25
87:1 88:20 90:21
91:11,18 95:9,9,17
109:18,23 113:20
114:6,8,11,19
132:6 140:6 184:7
185:1
**electronic**   18:4,9
53:12,16 54:8
60:25 61:5,16
62:9,16,18 63:3,14
63:17 70:1,15
73:10,15,19,25
75:1,15 79:23

81:17,21 94:25
95:6 101:16,19
104:6 163:1 164:4
181:21,23,24
**electronically**
69:16 75:14 82:11
**elements**   18:1
176:17,18
**elevated**   98:1
186:12
**eliminate**   87:8,22
88:1
**emergency**   74:2
**empirical**   156:2
**employ**   135:22
174:4
**employee**   194:19
**employees**   171:8
**ems**   122:17,23
135:22 150:12,19
150:24 169:21
**enabled**   82:14
**encode**   165:5,20
**encoding**   165:18
**encounter**   22:18
70:20 88:16 90:14
94:8 134:9 167:21
**encountered**   21:24
**encrypt**   23:3,11
**encrypted**   151:23
151:23
**encryption**   19:14
26:24 27:2
**endemic**   38:19
**endorsed**   34:23
**enet**   102:4,6,11,13
102:16,16,23
103:3,5,20,21,22
104:1,2,5,14,24
133:9,12 134:14
134:16,25 158:4

158:22,23 162:7
192:4,10
**engineering**   34:24
**english**   2:11
**ensured**   111:8
**enter**   66:10
**entire**   18:22 87:11
119:13 136:19
**entirely**   81:16,18
108:4 167:24
**entitled**   54:7
**environment**
38:25 158:22,25
**environments**
171:9
**equal**   98:7,16
181:6,6
**equation**   82:24
84:6
**equipment**   8:22
8:25 35:25 36:3
39:14 40:2,3,8,12
40:16 41:14 53:21
62:23 65:20 87:23
92:18 94:25 121:1
121:4,6,14 132:4,5
132:9 147:21
172:4 175:25
**erase**   117:6
**error**   40:6 156:7
**errors**   75:22 156:4
180:15
**especially**   14:5
44:16 133:23
134:12 171:13
**essay**   65:11,13,22
**essential**   33:10
78:17
**essentially**   21:16
27:4 38:13 82:9
113:17 140:16

142:9
**established**   180:14
**establishing**   70:15
**estimate**   12:8
115:17 138:3,4
156:5
**et**   1:5,11
**etcetera**   20:4
**ethical**   19:22
20:17 53:22,25
54:7,17
**ethics**   19:17
**evade**   150:5,16
**evaluate**   21:4
81:25 82:3 167:4
182:12
**evaluated**   81:15
81:22 102:22
103:1,19,20 118:1
138:11,13 168:25
182:9,13
**evaluating**   80:19
92:7,12 93:5
106:24 118:19
156:9 171:20
**evaluation**   85:12
101:22 172:5
**evaluations**   136:8
**eve**   160:24
**event**   66:18
**eventually**   76:14
157:24
**everybody**   7:10
**everybody's**   71:23
**everyone's**   71:16
**evidence**   39:18,21
40:1,7,10,16,23
41:1 42:20 44:7
44:13,16,17 53:19
53:19 58:10 62:22
63:7,11 66:2

[evidence - fair]

Page 15

112:19,22 113:14
113:17 114:7,17
117:9 121:3
122:12,18 129:3
130:19 131:20,24
132:4 134:16
135:25 153:6
156:7 159:4 162:9
162:12 169:2,7,10
178:14 181:7
188:1 190:21,22
191:8
**evident** 175:10,13
175:17
**evn** 4:6,7 24:21
25:7,16 27:15,17
28:1
**evolves** 148:24
**exact** 93:16
**exactly** 12:3 15:5
49:17 108:23
124:9 129:13
138:3 143:15
**examination** 3:5
6:19
**examinations** 3:1
40:11
**examine** 12:19
14:14
**examined** 6:7
14:10 101:15
158:21
**examining** 82:5
**example** 28:16
61:11,14 62:1
66:9 72:9 76:1
80:11 127:1,11
131:7 132:15
143:3 177:10
**examples** 90:23
95:11 99:18

113:22 172:11
**excepting** 81:19
**exciting** 18:11
**exclusively** 33:17
38:21
**excuse** 25:25
36:12 70:22 107:3
184:24
**exercise** 20:17
**exhibit** 4:2,3,4,5,6
4:7,9,14,18,20 5:1
5:5,8,11,12,15
9:20,23 10:5,7,16
10:19,22 14:20,23
25:3,6 27:11,13
29:24 30:2 37:1
37:13,15 43:20,21
52:5,7 54:11,12
55:1,3 56:22 57:2
60:8,9 67:22,23
69:7,8 76:17 97:6
97:7 182:23
187:13,13
**exhibits** 4:1 5:20
**exist** 151:6
**existence** 144:23
147:10 166:22
**exists** 83:11 131:5
**expect** 120:5
149:20
**expected** 147:6
**experience** 8:4
79:17 101:18
136:10
**expert** 4:4,5 11:10
12:14 28:5,7,11,15
28:22,23,24 29:12
29:15 89:11
**expertise** 28:5,19
28:24 29:14 92:7
124:20 163:7

**experts** 24:18
66:12
**expires** 194:25
**explain** 104:13
**explained** 186:11
**explanation** 57:22
**exploit** 151:3
152:11
**exploitable** 139:10
139:12 140:2
143:4,7 147:6
**exploited** 45:16,19
82:8 161:15
**exploiting** 139:25
**export** 104:5
**expose** 147:10
**exposed** 31:7
161:6
**exposes** 73:12
**exposing** 24:8
**exposure** 21:7,11
21:13
**expressing** 14:23
15:8,13
**expression** 134:6,7
**extend** 180:25
**extends** 150:23
**extensive** 46:13
175:12
**extent** 51:22
**extra** 172:1
**extract** 117:6
**extreme** 74:1
**extremely** 116:23
138:20 158:1

**f**

**face** 82:13 140:14
**faced** 107:6 110:7
144:20
**faces** 109:19 110:5
154:17

**facility** 169:18
**facing** 20:25 77:8
81:1
**fact** 32:22 69:21
71:20 86:9,16
89:19 106:22
119:12 127:19
142:15 143:11,24
144:5 150:8 152:9
153:7 155:8
167:19 168:8
177:13 180:16
186:2,5 190:23
**factor** 18:5 138:13
190:13
**factors** 49:25 50:3
50:8 118:18,21
**facts** 13:6 74:4
**fail** 50:24 167:9
178:11
**failed** 150:10
**failure** 39:14 40:5
40:8,16 179:6
**failures** 17:5 40:3
40:19
**fair** 1:5 14:25 19:9
19:11 24:9 29:4
31:5 38:6,7 40:4
50:7 53:5 55:13
56:5 59:10 73:9
73:11 74:5 77:8
77:19,22 80:5
84:25 89:24 109:9
112:15,16 115:13
115:24 125:13
128:10,11 129:10
141:15 148:5
162:23 171:18
175:18 176:8
181:17 185:6

Case 1:18-cv-05391-SCJ    Document 401-1    Filed 06/27/20    Page 212 of 243

J. Alex Halderman , Ph.D.

February 25, 2020

Fair Fight Action, Inc., Et Al. Vs. Raffensperger, Brad, Et Al.

**[fairly - fully]**

Page 16

**[function - going]**    Page 17

| | | | |
|---|---|---|---|
| **function**  38:9 | 42:25 52:16 71:1 | 158:22,23,25 | 151:5 152:9,18,19 |
| 63:24 140:7,8,9,11 | 95:19 152:25 | 159:8,11,22 163:8 | 156:5,22 167:5 |
| 173:5 | 176:11,16 | 163:15,20,24 | 194:15 |
| **functional**  158:19 | **generate**  44:17 | 164:8,12,13,19,21 | **global**  94:16 |
| **functionality** | 53:19 190:21 | 165:2,7,13,20,22 | **globally**  94:19 |
| 167:24 170:9 | **generated**  178:3 | 166:20 168:3 | **go**  7:1 10:2 12:16 |
| **functioning**  121:2 | **generates**  133:18 | 173:18,23 174:4 | 15:15 17:19 18:13 |
| 121:4 122:7 | **generous**  109:2 | 175:10 176:12,19 | 35:15 37:1 40:22 |
| 140:23 | **george**  67:4 | 176:22 177:22 | 46:12,23 47:11,21 |
| **functions**  102:10 | **georgia**  1:2,11 | 184:13,15 187:19 | 48:1 76:25 83:4 |
| **fundamentally** | 2:13 13:22,23 | 188:2,20 189:1,22 | 88:20 96:9 100:10 |
| 37:22 90:2 | 15:9,17,20,22,24 | 190:18 191:1,20 | 102:3 103:18 |
| **funding**  59:3,6,9 | 15:25 16:3,5 | **georgia's**  8:14 | 118:15 125:12 |
| **funds**  51:14 | 30:16 31:1 32:10 | 30:20 31:3 32:6 | 126:18 127:13 |
| **further**  35:4,9 | 32:11,18 33:23 | 32:13 47:15,17,18 | 128:21 129:9 |
| 48:1 129:9 130:18 | 50:17,20 51:1,3,19 | 47:24 48:8,10,13 | 130:25 142:17,23 |
| 142:18 153:5 | 59:6 64:25 65:9 | 49:1 50:10 77:7 | 164:22 172:11 |
| 160:12,14,15 | 66:23 76:7 77:17 | 77:20 79:11 80:18 | 174:20 178:22 |
| 166:1 170:5 193:3 | 81:3 90:22,24 | 80:25 100:19 | 182:14 186:24 |
| 194:16 | 91:5,8,9,24 93:4 | 102:6,23 104:4 | 191:2,3,16 |
| **future**  114:5,11 | 95:12,18 103:21 | 106:24 107:7 | **goal**  53:11 84:15 |
| 157:21 | 104:3 105:11 | 108:20 109:18 | **goals**  59:4 |
| | 107:23 108:3 | 114:22 117:10,16 | **going**  7:5,9 9:22 |
| **g** | 109:18 110:5,12 | 123:24 131:18 | 10:1,3,14 16:14 |
| **gain**  23:17 | 111:19 113:2,4 | 134:16 137:24 | 23:6 25:5 27:24 |
| **gained**  58:12 | 114:6,8,18 117:18 | 140:5 146:12 | 37:15 38:4 41:7 |
| **gaining**  152:6 | 118:3,6 120:10,14 | 149:3,16 152:1,23 | 43:20 47:4 55:1 |
| **gaps**  112:22 | 121:5,16 122:13 | 153:6 157:7,9 | 60:7 65:10 69:20 |
| **gems**  123:1,6 | 122:19 123:16,17 | 158:21 160:2,10 | 72:13 73:2 76:10 |
| 189:18,19,21 | 123:19 124:3,6,8 | 161:9 171:16 | 76:12 87:23 88:8 |
| 190:5,6,8,11 | 124:11 125:20,22 | 177:3,20 178:15 | 88:23 90:3,5 92:9 |
| **general**  4:13 8:5 | 125:24 131:5,17 | 178:17 190:15 | 93:10,13,14 96:8 |
| 16:3 19:21 22:2 | 132:6,9 134:12,21 | 192:15 | 97:5 108:14 109:8 |
| 22:15,16 29:21 | 134:25 137:4 | **getting**  33:1 59:6 | 120:22 123:25 |
| 38:2 43:10 53:13 | 142:14 144:20 | 79:23 | 126:1 127:18 |
| 64:25 73:22 76:16 | 146:6,8,10,23 | **gideon**  24:13,24 | 137:7,11 141:16 |
| 98:16 99:7 140:21 | 147:21 148:20 | **give**  12:18 54:9 | 142:17 144:22 |
| 145:4,4 147:11 | 150:18 151:7 | 99:18 119:17 | 151:24 153:18 |
| 148:24 177:23 | 152:6,9 153:10,22 | 137:11 184:14 | 154:24 156:25 |
| 186:8 192:4 | 153:23 154:1,5,10 | **given**  53:25 54:3 | 162:8 169:14 |
| **generally**  8:14,19 | 154:17,22 155:1,6 | 85:15 93:9 151:4 | 173:18,24 174:1 |
| 11:13,14,20 16:10 | | | |

Case 1:18-cv-05391-SCJ    Document 401-1    Filed 06/27/20    Page 214 of 243

J. Alex Halderman , Ph.D.    February 25, 2020

Fair Fight Action, Inc., Et Al. Vs. Raffensperger, Brad, Et Al.

**[going - higher]**                                                                Page 18

175:5,17 176:13
177:5,20 178:20
183:16 186:8
187:18 191:23
192:12
**gold** 142:6
**good** 6:21,22,23
6:25 56:10,14
76:11,14 77:23
89:6 90:19 94:17
100:11 111:17
117:22 134:8
135:4 141:14
144:8 174:8 176:5
179:23 183:4
188:22
**goodness** 187:20
**google** 175:22
**gotten** 84:7 97:16
147:21
**government** 4:13
29:21 54:2 112:3
115:1,12 116:2,13
117:15 140:5
169:19 171:6
**governments** 81:5
89:9 114:5,7,10
171:14
**grant** 51:14
**grants** 170:13
**grasping** 156:11
**gray** 157:6,7,8,14
157:16
**great** 66:16 90:25
91:25 117:23
**greater** 65:13
83:13 109:20
152:12 160:9
172:3
**ground** 7:1 164:2

**group** 22:23 24:17
35:8 38:10 66:14
96:18,23 182:12
**groups** 14:8 19:4
**growth** 18:6
**guess** 22:16 51:14
69:23 88:6 90:23
137:11,12 152:17
152:22 155:23
**guessing** 71:5
**gun** 41:6 114:15

**h**

**hack** 20:15 23:20
62:9,16 67:8
77:13 151:16
171:8
**hacked** 4:21 5:6
38:14 52:11 53:21
54:1 56:19 57:24
61:18 62:24 63:8
63:10 65:15 67:3
78:14 88:5 90:16
136:13,17,25
137:5,12
**hackers** 5:3 30:13
30:19
**hacking** 5:9 20:17
39:7 53:23 57:16
58:2 60:20 61:5
67:5,10 72:22
87:13,22 89:17,21
90:10 192:18
**halderman** 1:17
3:4 6:5,10,21 11:4
25:5,24 37:6 60:7
60:24 62:25 64:7
96:7 174:25 193:2
**halderman's** 4:9
4:14
**hand** 9:22 10:5,14
10:18 25:5 27:11

30:2 33:17 34:8
34:18 35:13 37:15
38:11,22 42:15
43:20 52:9 55:1
56:16 57:1 59:16
60:7 64:18,25
66:1,4 69:7 73:16
73:17 74:6,16
75:4,8,8,9,16,17
75:24 76:2,7
78:11 81:19,22
82:10 83:2 85:7
85:14,19 86:4,6,12
87:1 91:18 97:5
97:23 115:6,12,19
125:2 139:4
140:19 141:3
172:20 181:17
182:22
**handel** 16:19
**handful** 117:22,24
**handle** 71:10
109:8 131:8
**handling** 29:12
**happen** 23:23 77:7
78:2,3,4,6 81:10
81:11 94:20,21
103:11 169:6
**happened** 35:17
48:2 72:20 78:2
117:9 121:4
122:13,19,25
129:9 131:1 132:1
134:15 135:25
169:8,10
**happening** 51:19
51:21 129:25
171:17
**happens** 7:19,23
86:11 104:7
107:24 108:3,5

**hard** 74:3 129:24
**hardware** 98:4,9
98:14,14,16,17,18
141:13
**hash** 174:3,4,9,14
174:16
**hashing** 174:8
**hate** 131:16,16
**head** 94:3 144:14
150:2 182:8
**heading** 44:4
**headline** 58:15
59:14
**heard** 29:8 86:23
86:25
**hearing** 159:7
**heightened** 133:24
134:12 153:13
**help** 16:21 21:3,14
21:19,20 52:1
59:9 71:24 191:22
**helped** 16:2
**helpful** 124:21
**helping** 20:24 59:5
**helps** 20:2 21:6,10
153:8
**herman** 2:2 6:18
10:12,25 30:10
45:6 70:5 96:2
193:5
**high** 40:18 58:5
69:15 72:7 76:18
77:8,11 78:5 81:1
84:19 88:10 89:8
93:13,22 109:17
116:3 144:16
147:23 156:17
183:22 184:6,25
185:19
**higher** 116:5
117:18 137:22

**[higher - individuals]**
Page 19

144:11 148:25 169:17
**highly** 145:9 180:23 187:25
**hill** 43:1
**hillary** 66:8
**hired** 52:1
**hiring** 51:16
**history** 191:14 192:8
**hold** 69:4,10
**home** 45:15
**hone** 110:21
**honest** 171:8
**hope** 90:18
**hopefully** 151:25
**hoping** 15:6
**hospital** 20:15
**hospitals** 53:23
**host** 72:4 73:10
**hostile** 81:5 95:3 114:25 116:1,13 116:22 117:15 171:6,14 176:4
**hour** 11:6,20 33:2
**house** 4:10 29:20 127:12
**https** 23:6
**huge** 151:5
**huh** 7:13,13 176:17
**human** 17:23 18:1 40:6 97:18 103:11 103:12,15 104:20 125:10 126:8
**humans** 26:16
**hundreds** 23:13
**hypothetical** 72:14,15 81:18 85:14,15 166:24 167:12

**i**

**icc** 101:2,9 173:2
**icp** 101:2,6 107:20 138:5,6 173:2
**icx** 101:1,4
**idea** 141:14
**identification** 183:12
**identified** 14:2
**identify** 14:17 16:21 22:6,9 28:23 33:9 62:14 77:6
**identifying** 81:12 161:10
**identity** 23:5,9
**image** 189:11
**images** 172:19 173:17,19
**immediate** 57:13
**immediately** 46:25 162:7
**impact** 14:21 15:4 15:5,11 185:8
**impacts** 14:10,13 14:18
**impersonate** 120:13
**impersonation** 120:17,18,19,20
**implement** 124:17 124:22,24
**implementation** 100:20 146:5 165:14
**implemented** 110:12
**implication** 58:4
**implications** 19:22 53:22 54:1,7

**implies** 149:8 151:2
**imply** 51:24
**importance** 71:7
**important** 21:21 33:18 38:15 71:21 72:11,17 78:12,22 79:25 83:14 87:6 99:22 107:15 109:21,22 115:14 115:15 118:21 129:6 136:18 145:20,22 151:21 165:4,17
**imposed** 153:21 154:3 155:7 165:23
**imposes** 156:17
**impossible** 177:23 179:7
**improperly** 86:12
**improved** 110:15
**improvement** 36:21 39:2 185:1
**improvements** 51:15 53:13,15
**inadequate** 190:16
**include** 30:25 56:8 56:10 75:25 112:11 164:9 167:1 178:16
**included** 16:9 31:2 163:5
**includes** 49:1 112:8,10 142:5
**including** 30:15 33:15 34:23 35:8 36:3 42:2 81:1,23 90:19 122:3 142:11

**inconsistencies** 186:6
**inconvenient** 66:13
**incorrectly** 38:14 57:12 131:7
**increase** 120:5,9 170:3 183:18,21 183:24 185:4
**increased** 171:12 171:16,20 183:8 183:13
**increasing** 24:20
**independent** 33:20
**independently** 133:15 179:17
**index** 3:1
**indicate** 11:5,9 17:5 24:12 32:13 33:11 35:23 36:9 57:5 59:19 100:17 105:15,23 107:18 112:24 113:4 119:24 120:12 123:12 125:11 127:21 138:5,15 152:14 164:25 172:17 173:10
**indicated** 13:13 65:12
**indicates** 44:4 48:5,21 51:13 56:24 60:23 65:17
**indication** 49:8 70:13 112:4
**indicator** 144:8,8
**indirectly** 194:20
**individual** 63:12
**individuals** 15:23 16:1 129:17 161:3 182:16

**[induce - isrg]**                                                    Page 20

| | | | |
|---|---|---|---|
| **induce**  129:4 | 113:25 192:4,5,6 | 44:15 46:14 112:2 | 160:22 163:9 |
| **ineligible**  131:7,14 | 192:10,11 | 113:10 134:20 | **intervention** |
| **inert**  47:6 | **ingredients**  191:4 | **intended**  161:6 | 103:11,12 104:20 |
| **inevitably**  139:9 | **inherent**  43:5 | **intending**  115:6 | **interviewed**  60:16 |
| **infect**  135:22 | **initial**  135:15 | **intends**  173:23 | **introduce**  132:13 |
| **infected**  150:4 | **initially**  18:7 | **intensive**  147:23 | **introduced**  64:14 |
| **infecting**  190:6 | **inject**  149:7 | **intent**  38:17 85:25 | 132:3,5 149:1 |
| **infection**  135:15 | **inner**  158:20 | 113:9 140:13 | **introduces**  170:14 |
| 167:16 | 161:7 | **intention**  15:12,14 | **introduction** |
| **inference**  31:5 | **input**  105:6 | 15:15 | 106:4 132:11,12 |
| 134:23 | **insecure**  58:17 | **intentionally** | **intrusion**  132:10 |
| **inferior**  36:9,10,15 | 59:8 | 58:22 192:17,19 | **invalidate**  150:21 |
| **infiltrate**  46:8 | **insertion**  49:2,4 | **intentions**  36:24 | **inventor**  69:11 |
| 77:15 117:13 | **insists**  62:25 | 136:21 | **investigate**  20:10 |
| 160:19 170:8 | **inspect**  65:20 | **interact**  26:16 | 20:21 129:9 |
| **infiltrated**  169:3 | **inspected**  188:5 | **interchangeably** | **investigating**  17:5 |
| 190:5 | **inspection**  38:16 | 111:3 | 20:11 |
| **infiltration**  117:5 | 65:25 121:13 | **interest**  17:22 | **investigation** |
| 125:5 166:19 | **inspections**  66:4 | 69:19 83:25 85:24 | 30:23 130:18 |
| 167:7 189:22 | **install**  107:19 | 86:1,2,3 | 134:20 |
| 190:3 | 149:25 150:22 | **interested**  17:20 | **invited**  37:8,10,11 |
| **influence**  53:11,13 | 173:7 | 194:20 | **involve**  26:21 |
| **influenced**  169:15 | **installation**  149:5 | **interesting**  61:21 | 28:21 42:24 52:24 |
| **inform**  16:3 | 149:6,9 | **interests**  84:2,4 | 69:13 87:13,13 |
| **information**  13:13 | **installed**  123:8 | 87:3 88:19,24 | 122:2 167:6 |
| 15:17 16:8 44:10 | **installing**  108:23 | **interface**  104:10 | **involved**  11:17,17 |
| 48:18 65:14 71:8 | **instance**  20:13 | 165:6 | 12:12 19:22 42:25 |
| 104:15,23 120:13 | 33:25 39:4 55:22 | **interfaced**  103:6,7 | 43:3 46:7 52:17 |
| 130:25 133:12,13 | 74:1 75:21 82:22 | 103:8 | 55:24 61:24 65:24 |
| 133:22 134:10,10 | 90:20 92:14 | **interfere**  43:18 | 65:25 75:16 80:9 |
| 152:10 158:8 | 147:19 151:22 | 112:5 | 97:1 118:22 147:1 |
| 161:9,10,20,24 | 162:5 | **interfered**  41:14 | 147:19 152:5 |
| 162:2,3 163:4 | **instructions** | **interference**  112:6 | **involves**  34:3 |
| **informed**  15:21,21 | 174:15 | 112:11 | 146:14 |
| 16:2 | **insufficient**  173:22 | **interfering**  112:12 | **involving**  17:22 |
| **informing**  20:1 | **integrity**  25:2 | **international** | 43:17 |
| 107:1 144:19,24 | 181:19 | 61:24 | **iowa**  72:20,25 |
| 144:25 | **intelligence**  4:17 | **internet**  19:16 | **irresponsible** |
| **infrastructure** | 4:19 30:23 31:6 | 20:25 22:23 23:2 | 22:21 |
| 23:2 30:15 33:11 | 32:1,9 37:7,9,17 | 31:7 114:1 132:20 | **isrg**  22:22,23,25 |
| 41:13,18 43:14,18 | 40:20 43:16,24 | 133:5 134:5 135:6 | 23:1,11 24:2 |

Case 1:18-cv-05391-SCJ    Document 401-1    Filed 06/27/20    Page 217 of 243

J. Alex Halderman , Ph.D.
February 25, 2020
Fair Fight Action, Inc., Et Al. Vs. Raffensperger, Brad, Et Al.

[issue - leaves]
Page 21

**issue** 18:25 64:9
64:10 65:9 70:16
70:20,25 100:22
100:23 162:19,23
162:25 176:3
186:14
**issued** 23:12
184:17,19
**issues** 17:14 26:8
64:8,22 98:1
146:18 159:3,7
160:7
**item** 18:25
**items** 167:19

**j**

**j** 1:17 3:4 6:5
25:23 60:24
**january** 82:23
93:8 156:4 177:14
**john** 24:13,24
**josh** 25:22
**journey** 16:25
**judge** 9:9 67:6
**jump** 181:10
**jurisdiction** 38:21
85:5 124:23,25
127:10 162:5
**jurisdictional**
172:1
**jurisdictions** 41:4
79:4,6 115:18,21
115:25 122:10
124:16 131:23
145:21,22 154:18
154:23 171:13,13

**k**

**kadel** 181:14
**keep** 5:2 59:2
76:11,12 100:5

**kennesaw** 189:12
**kept** 100:3,5 121:4
**kerckhoffs** 99:24
**key** 36:21
**keys** 100:8 151:3
**keyword** 59:25
**kind** 8:2,4 16:24
18:3 19:21 21:12
33:1 44:2,17
50:18 56:2 58:7
66:20,23 70:17
72:22 75:19,20
79:7,12,24 80:2,10
94:19 99:13
100:13 102:16
109:12 111:3
114:21 115:20
118:18 122:23
123:10 124:15
126:19 127:22
131:24 132:8
146:15 147:24
148:14,21 152:10
152:21 167:10
172:3,5,11 176:6
180:5 183:12
184:9 188:18
**kinds** 36:15 43:11
53:23 59:14 72:3
73:13 95:13 105:8
106:9 175:14
176:2 177:6
179:10
**know** 5:5 7:8,21
7:22,23 12:1 17:1
17:12 18:2 27:24
28:2 31:25 32:17
34:25 41:12,15,20
41:20 45:1,9
48:16,19 49:1,14
51:20 61:10 62:13

62:17 63:9 72:14
74:13 75:10 95:1
102:11,14 104:5,7
104:22,25 106:1,7
106:10 107:8,21
108:1,13,23 109:3
112:17 113:21
119:4 120:11
121:22 123:9,24
125:21,23 126:20
127:17 129:24
131:11,25 133:11
134:25 135:2
137:6 138:2
144:13 148:18
149:15 150:6
151:6 152:4
153:21,23 157:9
159:6,22 160:2
163:15,17,22
164:15,21,24
165:2,4,13,16
173:18 174:5,7
178:19,19,23
179:16,19 180:7
181:25 182:7,8,8,9
184:15,16 189:20
190:20
**knowink** 100:22
169:4
**knowledge** 15:22
16:3 32:12,21
41:1 79:12,16,25
80:2 81:9 97:22
101:23 119:12
121:8 132:7
148:17 153:25
159:5 161:4
164:13,19 178:8
**known** 22:18
34:14 58:17 143:3

143:12 144:6,12
144:13 171:23,24
171:25 174:8
176:22
**knows** 23:9
**kurt** 9:12

**l**

**lab** 116:7,11,16,17
126:2,6
**labeled** 66:12
**lack** 28:24 110:9
110:16,17,17
140:11 153:11
**landscape** 155:19
**language** 138:16
**languages** 138:23
138:24
**large** 11:17 19:12
41:18 51:24 65:24
74:23 139:11
179:2,6
**largely** 110:9
**larger** 184:1
186:22,24
**largest** 23:11
**late** 130:22 131:11
**law** 123:16,17,19
131:5 184:15
**lawful** 20:3,5
**lawmakers** 55:10
**lawsuit** 12:12
**lawyer** 70:10
**lawyer's** 187:7
**lax** 145:11
**lead** 71:24 117:17
153:13
**leads** 34:12 71:9
136:4 139:12
**lean** 27:25
**leaves** 159:21

J.  Alex Halderman , Ph.D.                        February 25, 2020
Fair Fight Action, Inc., Et Al. Vs. Raffensperger, Brad, Et Al.

**[led - malware]**                                                        Page 22

**led**  18:25 35:9
  91:5 159:18
  171:16
**lee**  15:25
**legal**  13:18 51:7
  125:25
**legislation**  49:23
  64:23
**legislative**  55:16
  55:17
**lenawee**  194:4,24
**lesser**  83:13
**level**  22:18 49:14
  50:3,19 55:21
  72:8 76:18 80:1
  81:14 87:16,17
  88:15 99:11
  107:12 109:4,19
  109:20 114:23
  115:11,25 116:11
  118:17 129:5
  139:22 144:9
  147:23,24 152:8
  155:4,20,22 156:1
  156:18 160:15
  162:15 166:2,12
  167:4,21 168:4,10
  168:22 192:6
**levels**  155:24
**license**  21:12,18
**lies**  19:6
**light**  178:14
**likelihood**  156:3
  184:25
**liles**  45:3,9,11
**limit**  42:6 50:4
**limitation**  36:21
**limitations**  27:9
  36:22 109:11
  113:14 165:2,3,22
  171:3

**limited**  81:3 100:7
  145:24 146:15
  147:5,16 148:1
  158:12,14,15,16
  158:17 175:3
  178:25
**limiting**  34:14
  49:13,15,20 50:11
  50:14,18,23 51:2
  78:12 123:21
**limits**  44:14
**line**  18:16 60:23
  70:11
**lines**  39:15 88:23
  89:6 91:13 128:20
  137:18,21 138:5
  138:10 139:11
  140:8
**link**  70:15 71:3
  168:17
**linked**  62:2
**list**  19:8 27:20
  77:19 82:12,20
  132:11 143:3
  164:4,4
**listed**  25:20
**listen**  57:8
**literature**  111:2
**litigation**  12:13
  16:11,12,14
**little**  12:11 16:24
  17:8 26:4,25 28:4
  49:7 65:10 76:10
  76:12,15 105:13
  132:18 133:7
  184:21
**live**  162:2
**lives**  17:23
**llp**  2:11
**locally**  175:20

**location**  169:19
**log**  71:6
**logic**  177:1,2,4
**long**  30:9 39:15
  54:19,20 75:9
  88:23 89:6 128:20
**longer**  53:21 72:11
**look**  5:7 33:16
  34:5,10 60:19
  70:10 82:16 92:14
  124:17 181:12
  190:2
**looked**  8:20 63:8
  118:13 133:15
  149:14 189:21
**looking**  18:2,16
  25:25 34:5,13
  36:2 45:15 47:10
  67:13 77:1 84:24
  85:6 93:24 182:7
**loss**  152:25
**lot**  23:23 34:23
  36:2 71:9 94:4,21
  111:10 115:22
  128:17 151:19
  174:9 179:24
  185:3,4
**low**  93:15,21
  180:15,16
**lower**  110:20
  144:11
**lunch**  76:13 94:17
  96:7

**m**

**machine**  44:21,23
  47:4 62:10 66:18
  66:20 67:3,13
  69:25 75:22,23
  95:7,19,21
**machines**  15:10
  37:21 39:14 40:25

  43:11 44:8 47:4
  48:6 52:24 53:1
  53:16,18 56:10,14
  58:17,20,21 59:2,9
  61:5 62:23 63:4,8
  63:10,12,14,17
  73:16 95:8,12,14
  95:17,25 157:2,7,9
  186:9 187:16
  191:5
**magazine**  57:12
  60:12
**magnitude**  183:24
  184:1
**mail**  105:16
  120:16,18,23
**mailed**  37:11
**main**  27:21 59:14
  67:14 77:20
  102:17
**maintain**  71:3
  178:8,21
**maintained**  135:3
  142:1 192:19
**maintaining**
  118:23 121:13
  142:6
**maintains**  134:25
**maintenance**
  145:2
**majority**  184:4
**making**  47:10 99:1
  107:10
**male**  171:8
**malicious**  5:17
  52:25 78:24 132:3
  134:17 170:9
  179:3
**malware**  123:4
  126:2,7 132:2,5,10
  132:11,13 135:18

Veritext Legal Solutions

Case 1:18-cv-05391-SCJ    Document 401-1    Filed 06/27/20    Page 219 of 243
J. Alex Halderman , Ph.D.
February 25, 2020
Fair Fight Action, Inc., Et Al. Vs. Raffensperger, Brad, Et Al.

[malware - method]

Page 23

150:4,9,16,20
172:18 173:4,7
174:14 177:12,15
190:6,13
**man** 66:17 147:22
**manage** 104:1,3
**management**
101:13 132:15
170:10 179:5
180:4 189:20
**mandela** 61:15
**mandela's** 61:20
61:23
**manifested** 84:4
**manipulate** 32:3
172:19
**manipulated**
31:13,16 44:8,22
44:24 112:19
**manipulating**
30:14 31:23 46:21
112:11
**manipulation** 5:17
80:9 89:17 90:10
112:7 113:7
122:16 189:23
**manual** 34:22
65:25 66:3 75:15
123:15
**manufacturer**
135:12 142:10
172:24
**manufacturers**
20:1 149:24
**map** 57:18,19
**margin** 186:14,20
186:22,24,25
187:1
**marilyn** 181:14
**mark** 7:10,11,21
10:2 64:13

**marked** 9:20,22
10:5,7,16,18 25:3
25:6 27:11,13
29:24 30:2 33:17
34:8,18 35:13
37:13,15 38:11,22
43:20,21 52:7,9
55:1,3 56:16,22
57:1 59:16 60:8,9
64:18,25 66:1,4
69:7,8 70:4 73:16
73:17 74:6,16
75:16 76:7 78:11
81:19,22 82:10
83:2 85:7,14,19
86:4,6,8,12 87:1
91:18 97:5,7,23
115:6,12,19 125:2
139:4 140:19
141:3 172:20
181:17 182:22,23
183:19
**marker** 73:19
**marking** 5:18 26:8
33:15,18,22 34:9
34:18 35:2,6,10,14
36:10,16,17,18
42:2,7,8,11,14,15
42:17,21 43:12
59:21,24 60:2
65:1 73:17,20
82:11,16,22 83:1
86:4 91:1,19 93:7
93:17 97:22 98:2
101:1,4 138:1
145:16,18,23,24
146:1 149:18
152:24 153:2,5
156:15 166:23
172:20 175:11
176:19 177:3,14

177:21,25 178:3
180:1 181:12,25
184:10 185:22
188:13,15
**marks** 97:19
181:14,16
**marriage** 194:17
**massive** 41:10
148:6
**match** 38:17
**material** 8:10
12:24
**materials** 13:16
**mathematical**
178:6 185:21
186:16,19
**matter** 16:11,16
16:17,19 72:12
92:10,10 106:14
106:18 151:15,19
175:4 177:4
181:21 189:4,10
194:21
**matters** 94:10
105:8 128:17
155:22
**meadows** 64:13
**mean** 25:25 41:7
51:24 54:2 63:18
63:25 67:20 73:1
73:17 74:20 79:16
81:18 87:10 89:7
95:3 103:7,9
113:6 128:17
136:16 147:7
154:14 186:22
**means** 23:4 61:16
76:8 122:3 147:14
169:13 194:12,13
**meant** 161:19

**measurable**
185:11
**measured** 185:2
**measures** 33:10
63:19 151:16
167:8 172:9
**mechanisms**
121:18
**media** 66:7 112:13
135:7,11,14,16,20
**medicine** 34:25
**medium** 5:5 56:19
57:3 65:11,13,22
97:20
**meeting** 66:17
**meetings** 42:25
**members** 43:2
**memoirs** 61:25
**memorial** 24:13
24:24
**memory** 107:19
108:1,24,24 109:8
**mention** 38:10,18
59:14 108:5,10
170:2 174:25
**mentioned** 75:24
**mentioning** 59:3
**mentions** 67:2
**merely** 66:13
112:12
**mess** 73:8,8
**messages** 112:13
**met** 6:23
**method** 23:19
69:25 70:14 71:6
74:7,17 81:25
82:3,5,20,24 85:7
85:11 87:19 91:23
92:1 106:13,21,25
107:3,8,9,11
108:11 135:22

Case 1:18-cv-05391-SCJ    Document 401-1    Filed 06/27/20    Page 220 of 243
J. Alex Halderman , Ph.D.
February 25, 2020
Fair Fight Action, Inc., Et Al. Vs. Raffensperger, Brad, Et Al.

[method - newspaper]
Page 24

173:18 174:4
**methodology**
84:13
**methods**  14:25
15:3 27:3 29:10
80:10,16 84:22
127:1 129:7
132:11 141:10
**michelle**  25:23
**michigan**  1:19 5:8
5:16 6:1 18:14,15
18:20,23 19:1,2,2
21:23 58:13 60:11
65:25 67:20,25
81:24 117:23
119:1,4,5,8,15,16
119:21 182:21
194:2,6,24
**michigan's**  118:11
**microsoft**  25:23
**middle**  64:1 178:2
**midterm**  182:21
**milchev.com**  2:7
**miller**  2:3
**millions**  23:14
**mind**  80:17
**minimal**  65:19
87:16,18,20 88:8
**minimum**  87:17
**minute**  36:13
110:22 112:4
128:16 192:22
**minutes**  33:3 37:2
**misbehavior**
177:25
**misspoke**  17:10
**mistaken**  189:14
**mitigate**  21:14,21
22:5,12,14 119:8
121:23 125:16
159:2 170:15

**mitigated**  22:10
118:25 128:7,12
128:17,24 159:9
159:16 160:8
**mitigation**  160:3
160:13 173:21,22
184:6
**mix**  72:12
**mock**  67:3
**model**  21:1,12,18
21:19 95:20
**modeling**  166:17
**models**  166:21
**modern**  141:22,22
**modes**  167:7
**modified**  59:20
60:1,3
**modify**  149:8
**modules**  141:6
**moment**  67:19
**money**  58:19 90:3
160:17
**month**  178:17
**months**  123:10
159:6
**morning**  6:21,22
**move**  8:3 33:17
52:3 59:8 73:6
76:19 158:3 163:1
169:1 179:24
184:20,22 187:16
192:8
**moved**  38:22
188:16 191:15
**movement**  188:16
**moving**  168:9
**mueller**  134:19
**municipalities**
39:23 46:9
**murder**  63:23

**mvp**  103:1,4,13,19
104:10 133:7,8,11
133:11,11 160:23

**n**

**n**  21:9
**name**  21:8 25:22
71:16
**named**  63:24
**names**  182:16,19
182:20,20
**narrow**  100:8
**nation**  109:23
110:6,14 116:22
116:23 139:24
143:23 145:19
175:6
**national**  34:24
35:1,3,11 90:18
180:6,13 181:3
188:9
**nationally**  115:23
**nature**  134:7,13
**nearly**  101:18
**necessarily**  31:11
31:12,13 46:20
67:1 86:6 90:5
113:6 127:17
130:8 147:5,15
166:5 185:11
**necessary**  63:19
114:24 115:10,11
116:1,12 129:5
179:1
**need**  55:10 59:3,10
71:13 72:6 99:7
99:22 100:4,5
114:12 127:3,17
131:25 136:19
137:5 155:12,12
167:15 185:3

**needed**  57:10
142:17 151:3
185:4,14
**needing**  59:1
**needs**  118:7 139:6
191:20 192:8
**negative**  147:12
**negligently**  192:19
**nelson**  61:14
**network**  24:16,17
27:22 61:18 192:4
192:10,11
**network's**  24:13
**networking**  47:6
**networks**  45:18
**never**  21:23 39:8
41:20 113:11
140:25 146:17
149:10 152:25
180:10 187:18
188:19 191:23
**new**  4:20 5:13
18:10 35:15,22
47:16,17,18 48:9
49:1 52:6,10,13
53:2 54:22 57:11
77:22 82:7 97:2
97:10,13 100:20
109:18 110:2,7
114:22 121:6,10
121:19,21 122:19
122:21,21 124:1,2
136:3 137:4
141:18,19 142:16
170:14 175:11
177:3,21 180:24
**newer**  144:4
**news**  66:7 73:2
100:11
**newspaper**  71:17
71:23

**[nick - order]**    Page 25

**[order - part]**    Page 26

124:18 127:18
131:25 140:23
155:15 184:23,24
186:13
**organizations**  4:8
27:16,17,18,21,25
28:3
**originally**  96:24
**ought**  58:6
**outcome**  14:7
38:15 50:25 62:5
83:3 84:18,20,23
87:24 88:22 90:18
91:6 114:10 115:9
123:23 137:7
140:24 157:1
**outcomes**  122:18
190:17,18
**outdated**  141:5
142:25 180:2
**outline**  79:18
125:1 128:6
186:19
**outlined**  39:19
79:8,18 121:24
128:12 129:16
130:20 160:4
183:7 185:20
**output**  93:22,22
**outside**  94:11
160:4
**outwardly**  191:9
**outweigh**  84:5,9
**oven**  133:4
**overall**  15:22 59:7
83:19 103:10
105:1 107:15,17
154:8 157:13
168:16
**override**  64:22

**overseas**  169:12
**overvoting**  76:1
80:11
**ovr**  103:1,4,13,19
104:11 133:7,14
133:16 161:22

**p**

**p**  2:10
**p.m.**  25:13 193:6
**pad**  101:16 163:3
163:6 165:5,10,15
165:18,19,21,25
166:22 167:20
168:9
**pads**  8:22,24 163:9
163:16,19,24
164:14,23 165:1
166:12,23 167:17
168:4,14,16,17,22
**page**  3:3 4:2 10:21
25:9,10 33:9
34:21,21 35:23
36:6 37:19 38:18
39:11,12,12,19
41:11,22 44:3
45:2,5 46:12,12,23
46:25 47:10 48:5
51:12 54:14,15
55:8,9 57:5,17,18
58:14 60:20 62:20
63:21 64:1 65:10
67:1 69:24 70:2,3
70:7 77:3 100:12
105:15 112:24,24
161:24 179:13
**pages**  8:12 70:8
**paid**  24:1,4 68:13
68:14
**panel**  25:18,21
26:1,3,5,7,7

**panelist**  25:20
**panels**  25:16
**paper**  28:17 29:9
29:13 33:13,17,19
34:3,4,5,6,6,8,11
34:13,21 35:13
36:7,9,11,23 38:12
38:22 41:25 47:5
48:22 49:2,5
53:17 54:7,16
56:11,15 59:15,16
59:17 64:18,25
69:16 70:15 73:16
73:18 74:6,17
76:7 78:11 80:10
81:16,19,22 82:10
83:6 85:8 86:5,6
86:13 91:19 93:5
93:7,23 97:19
108:5,11,14,17
109:6 110:18,23
110:24,25 111:11
115:7,12,19
123:15 125:2
127:23 128:5
136:20,20,21
139:4 140:12,12
141:3 163:20
164:4 173:16,19
173:24 178:6,18
179:11,13,15,16
181:17 185:13,20
**paperless**  33:13
34:2 36:19 56:9
56:14 79:5 111:16
111:18 181:24
**papers**  54:4 92:25
93:24 94:4,11
**paragraph**  11:4
30:12 31:17,17
37:20 38:18 39:12

41:11 44:5 56:9
57:19 58:15 59:13
59:19 62:21 63:21
64:2,6 65:17 66:6
76:25 77:5 79:19
100:12,17 102:3
103:18,25 105:14
105:23 107:25
109:15 111:20
113:4,22 114:4,21
132:2,18 133:3
134:3 135:5 136:5
136:12 139:8
141:5 142:25
143:6 144:17,19
146:8,21 147:4
148:14 149:5
150:3 151:1 152:3
153:18 158:9
159:1 160:19
163:2,18 164:12
169:2,11 170:19
172:9,17 173:10
174:12,25 175:9
177:19 178:7
180:1 181:10
182:14 185:24
187:10,12,14
189:18 190:14
**paragraphs**  39:19
70:22 77:1
**parallel**  177:19,21
177:24
**pardon**  48:12
**parkwood**  2:12
**part**  15:16 19:18
26:8,10 29:6
52:12 53:10 56:7
59:7 66:15 72:25
84:6 93:8 103:4
107:1 108:18,25

**[part - point]**                                                    Page 27

137:3 139:6
141:21 142:14
146:13 147:18
154:7,7,8,13,14,15
156:2 167:13
168:4 186:5
**partial** 65:15
**partially** 58:13
**participated** 24:21
52:20,22 53:6
**participating**
27:17,19 52:13
**particular** 14:25
15:9 17:16 18:25
20:4,6 65:9 70:14
70:19 76:22,24
84:1 88:22 122:11
143:9 144:1
149:24 156:8
**particularly** 36:22
85:6 99:14 138:17
158:15,17 186:14
**parties** 161:15
194:18
**partisan** 64:7,9,10
64:16,17,21,24
65:4,5,8 66:9
122:11
**partisans** 66:13
**parts** 31:6 65:24
65:25 99:22
**party** 61:20
**passed** 55:22
**passwords** 151:3
**patent** 5:11 69:4
69:10,13,20 70:10
**path** 56:5,7 91:10
91:12,24 134:1
165:19 166:22
167:2

**paths** 166:17
**pattern** 46:7
**pay** 36:1
**pcc** 158:11,12
169:4
**peer** 179:15,17,20
182:3 184:8
**penetrate** 41:13
**penetrating** 30:13
**pennsylvania** 8:24
67:25 118:14
119:1 165:9,17,24
166:13,21,25
167:24 168:11
**pennsylvania's**
168:21
**people** 15:20 16:2
20:10,16 91:7
94:7,8 99:5
105:16 111:2
120:6 131:7,14
143:18 177:11
182:1
**percent** 58:1,3,5
115:21,24 116:3
156:19
**percentage** 93:16
115:17 116:4
**perfect** 8:1
**perfectly** 56:1
83:12
**performed** 49:24
50:21 67:6,7
164:13,15,16
**performing** 146:9
**period** 18:5 121:7
**permanently**
163:16
**permission** 20:14
**person** 71:4
105:19,22 120:18

120:20 133:19
153:12
**personal** 32:12,21
73:6 91:13,15
101:22 113:19
136:9
**personally** 56:13
95:13 101:3,6,9,12
101:15 102:25
158:21 163:2
**perspective** 18:2
74:9,11,16,19
75:12 77:21 91:7
98:13 185:21
**ph.d.** 1:17 3:4 6:5
17:10 183:3
**philip** 179:13
**photo** 120:14
**phrased** 44:13
**physical** 25:9
26:22 33:9 38:16
69:24 70:3 121:8
121:17,22 122:1
151:1,4,6,8,9,11
151:14,19,20,21
151:25 152:2,2,5,6
152:8,9 173:7,16
173:24 175:16,18
176:12,18,19,23
**piece** 29:2 34:12
59:17 67:18,20
99:11 102:12
114:22 126:6
132:8 140:2,25
143:13,16,17
144:7,22 160:21
170:4,6,7 177:9
**pieces** 8:2 71:8
76:19 92:17 100:4
132:19

**pilot** 50:14,15,18
123:21,23
**piloting** 124:21
**pirate** 169:24
**place** 40:12 41:2,3
77:18 78:23 87:15
87:22 108:3 121:1
121:3,18 128:20
140:25 145:3
162:11 176:25
**placeholder** 52:5
**places** 29:10 58:25
191:6
**plaintiffs** 1:6 2:8
8:11,11 9:13
12:15,22 13:2,5
15:18 102:2
**plan** 12:6,7 124:4
**planned** 125:20,21
**plans** 123:24
178:15,24
**plant** 171:7
**platform** 56:18
103:3
**plausible** 56:7
93:14 105:3,9,10
129:20
**plausibly** 139:20
**play** 64:16 84:2
**player** 102:18
**players** 102:17
**please** 26:25 127:8
187:6
**plenty** 95:8
**point** 15:7 21:20
34:21 35:11 48:7
49:18 54:6,9 61:8
61:11 62:11 64:9
64:10,17 65:13
71:5 76:13,14
88:10 89:1,2

Case 1:18-cv-05391-SCJ   Document 401-1   Filed 06/27/20   Page 224 of 243
J.  Alex Halderman , Ph.D.
February 25, 2020
Fair Fight Action, Inc., Et Al. Vs. Raffensperger, Brad, Et Al.

[point - primarily]

Page 28

91:25 92:3,4,5
94:17 98:1 109:16
132:21 136:18
138:21 148:5
156:18 158:2
165:14 175:2,4
178:1 189:6
**points** 41:22 44:5
163:14
**policies** 84:24
**policy** 55:10,12,19
59:4,11 63:19
72:12 74:25 83:19
84:9,12,15,20,20
84:23 85:4,4,18,20
85:24,25 86:2,3
87:3 88:14,17,17
88:24 89:1,7,9,10
92:18,21 94:10
134:9 148:3,8,12
164:8 181:21
183:16
**policymakers**
53:11 83:25 90:25
91:9,24 93:4
**political** 55:15,17
55:24 66:14 68:15
68:18,23
**politically** 56:5,7
**politics** 28:2 64:16
64:18,21 65:8
66:9
**poll** 8:22,24
101:15,16 104:6
163:1,3,3,6,9,16
163:19,24 164:14
164:23 165:1,5,10
165:15,18,19,21
165:25 166:12,21
166:23 167:17,19
168:4,9,13,16,17

168:21 184:13
**polling** 29:10
40:12 58:4 65:14
87:15,22 108:3
121:1,3 126:22,25
127:11 128:20
191:5
**polls** 57:20,22
163:12
**port** 151:2
**portion** 65:11
179:9
**position** 39:13,16
42:11 58:20
144:18 145:8
180:9,11 183:17
**positions** 42:14
97:13 98:1
**possibilities** 58:8
**possibility** 15:2
44:24 63:10
**possible** 38:1 51:1
51:3 55:24 71:25
72:22 75:5 80:20
81:12 82:7,13
85:2 87:7,15,21
88:1 94:4 109:5
126:20 129:4,14
147:16 149:7
150:5 157:21
162:3 164:14,16
177:12 178:20
179:3 189:8
**possibly** 84:24
94:20 128:13
164:1,9
**post** 5:1 18:3 49:9
49:10 50:1 54:23
55:5 179:9
**posted** 67:2

**posture** 32:17
145:9 154:9
157:13
**potential** 14:20
20:21 23:24 26:20
50:24 52:25 76:3
78:8,14 79:13
80:3,9,19,22
117:21 119:6
**potentially** 39:17
76:4 90:12 94:20
117:4 122:8
126:23 134:1
151:12 161:7
171:14 174:17
179:10
**power** 87:11
**powers** 89:17
90:10
**practical** 84:15
**practically** 84:4
**practice** 104:4
124:22 139:13
141:7,8 145:5,11
145:21
**practiced** 174:14
**practices** 13:22
15:10 28:16 29:16
34:22 141:23
145:1
**prayer** 187:5,7,9
**pre** 50:1 57:20
126:22 178:9
**precautions**
133:24 155:16
**precinct** 95:21
101:2,7 138:8,11
138:12 139:4
149:19,21,22,25
163:21,21 175:5

**precisely** 111:2
**preconditions**
115:10
**prefer** 74:21 98:13
98:15
**preferences** 97:20
**preferred** 20:18
98:8 99:16
**premise** 83:9
**preparation** 63:22
**prepared** 8:21
12:10 124:9
**preparedness**
162:16
**preparing** 12:2
**presence** 174:13
194:12
**presidency** 68:24
**president** 55:23
68:9 111:24
**presidential** 62:24
113:24 131:17
**pretend** 23:21
**pretty** 58:5 65:5
71:5 83:17,18
84:20 109:15
140:1 144:16
**prevent** 116:21
121:1 151:9
**prevented** 110:4
119:25
**previous** 95:12
137:24 159:17
180:22 188:23
**previously** 34:25
43:25 152:17
**primarily** 26:20
80:7,12,14,23
96:21,23 100:13
108:8 140:19

Case 1:18-cv-05391-SCJ    Document 401-1    Filed 06/27/20    Page 225 of 243
J.  Alex Halderman , Ph.D.                February 25, 2020
Fair Fight Action, Inc., Et Al. Vs. Raffensperger, Brad, Et Al.

[primary - publicly]                                                    Page 29

**primary** 16:2
70:13 76:8 168:18
168:18
**princeton** 17:1,18
18:12 19:1 69:21
**principle** 98:6
99:8,21,24,25
100:9 111:6
**principles** 5:13
19:21 97:2,11,18
98:3,22
**print** 71:16 125:6
179:1
**printed** 60:3
126:11 128:2,9
130:15 178:9
180:15 181:13
**printing** 71:23
171:10
**printout** 52:10
**prints** 59:17
**prior** 7:17 41:5
47:1 106:3,5
107:20 181:2,2
**privacy** 70:17 71:1
**privilege** 6:16
**pro** 11:24 68:12
**probability** 88:11
93:11,13 184:6
**probable** 132:9
**probably** 16:1
20:16 22:1 29:5
46:22 57:21 58:6
61:6,10 62:17
71:5 76:14 92:14
94:17 98:7 109:21
116:6 117:16,25
120:8 129:11
138:2,3 139:23
155:21 156:12,14
157:3

**problem** 16:24
41:2 72:4 142:14
143:9,15 151:4
152:11,13 179:2
180:24 183:24
186:23
**problems** 14:2,4
14:16 17:21,22
18:11 26:20 36:17
62:18 72:5 73:3
73:10 77:20 99:4
110:16 118:24
134:13 152:14,21
153:17 180:25
181:8 186:2,6,10
**procedure** 6:14
124:22,25 185:7
**procedures** 110:13
154:1,1 176:23
**process** 35:16,17
63:22 65:21 75:2
86:23 88:23 89:2
91:5 103:17
105:22 106:2,3,5
106:11 120:2
131:2 142:5
159:16 163:11
164:10,11 166:11
169:3 171:2
172:12,13 174:16
174:16
**processes** 104:19
124:12
**produce** 21:6 35:7
39:5 131:24 179:8
**produced** 8:10
172:4
**product** 141:19,20
**products** 27:6,7,10
**professional** 91:16

**professor** 18:17,22
60:23
**profile** 60:11
62:20
**profit** 22:24
**program** 135:24
165:5
**programing**
138:24
**programmed**
86:20 140:9 180:3
**programmers**
169:13 170:21
**programming**
105:25 135:11
138:16,23
**progress** 159:14
**progressive** 27:22
**prohibit** 167:24
**prohibition**
165:18 167:1
168:1
**project** 27:23
**prompt** 184:18,20
**prompting** 183:8
183:11
**prompts** 183:25
184:14 185:2,5
**promulgated**
154:2
**proper** 109:9
110:12
**properties** 157:22
**proportion** 82:25
**propose** 120:25
**proprietary** 98:19
**pros** 99:15,17,18
99:19
**protect** 33:10
175:6 176:2

**protected** 102:21
**protecting** 91:7
176:7
**protection** 90:2
102:22 150:5
152:8 167:8 175:2
175:4 177:6
**protections** 64:14
78:16 176:25
**protocol** 177:5
**protocols** 26:11
27:1 151:20,21
177:2,20
**prove** 147:11,12
147:13
**provide** 11:10,13
12:22 13:2 27:3,6
27:7,10 33:19
51:17 66:2 92:9
117:2 143:19
175:17,20 177:5
**provided** 8:11
12:24 102:2 163:5
**provides** 24:5
175:2
**providing** 12:13
188:8
**provision** 131:8
**provisional** 120:2
120:6 128:13,14
129:17
**provisions** 131:5
**public** 42:25 52:4
69:22 94:10
161:10,13 177:22
194:1,6,24
**publically** 154:1
158:7
**publication** 60:17
**publicly** 106:12
125:23

Case 1:18-cv-05391-SCJ    Document 401-1    Filed 06/27/20    Page 226 of 243

J. Alex Halderman , Ph.D.    February 25, 2020

Fair Fight Action, Inc., Et Al. Vs. Raffensperger, Brad, Et Al.

**[published - recognize]**

**published**  35:21
53:24 54:4 82:23
92:12,25 93:5,7,24
94:3 177:14
184:12
**pull**  31:20 41:7,9
114:18
**pulling**  114:15
**puppeteer**  66:8
**purchase**  47:3
121:19,21
**purchased**  48:6
**purpose**  6:12 34:7
34:11 164:9
**purposes**  6:13
12:23 14:9,11
108:13 133:22
176:6,7
**put**  15:7 77:17
88:6 133:22 148:4
187:13
**putin**  41:8 111:24
**putting**  39:15

**q**

**qualified**  109:7
119:18
**qualifiers**  95:1
**quantifiable**  88:11
88:21 148:1,2
156:9
**quantified**  118:6
172:7
**quantify**  93:9,15
172:8
**quantitative**  82:24
94:1
**quantities**  178:9
178:21
**question**  7:9,10,11
7:17,20,24 22:8
27:21,24 35:5

39:24 40:5 49:23
62:7 73:5 74:18
82:18 84:13 85:2
85:16,17 88:18
92:6,8 94:9 95:15
111:4 116:24,25
117:22 127:8
130:11 140:14
147:18 151:22
157:12 162:22
166:10 173:25
181:5 183:21
184:9 186:18
187:3,10 188:22
189:7 191:6,22
**questions**  17:3,18
19:18,25 20:2
44:2 55:20 66:11
84:12 94:16 112:3
192:14 193:3
**quick**  20:7
**quickly**  68:25
**quite**  30:6 93:19
94:4,9 142:22
151:10 157:4
**quote**  45:12,21
139:14
**quoted**  45:13
**qvf**  119:18,19,20

**r**

**race**  126:18,21,23
127:10,12,12,12
127:14
**races**  126:25 127:1
182:6
**racial**  14:1,5,8,10
14:12,14,20,24
15:4
**racially**  14:17
15:10

**raffensperger**  1:8
6:12
**raise**  15:2
**random**  178:1
**range**  51:24
157:18 159:2
160:7
**ranked**  19:3 118:5
**rate**  11:6,10,20,25
148:25 164:1,3
177:11 180:14,20
181:11 184:22,23
185:20 186:11
**rates**  185:8
**rattled**  45:17
**rattling**  46:10
**rdr**  1:22 194:24
**reach**  113:15
**reached**  100:15
**reaching**  80:18,25
81:7 85:9 107:6
108:19 109:1
176:20
**read**  13:8,10,13,16
13:16 62:22
103:17 125:8
128:6
**readable**  97:19
125:10 126:8
**ready**  8:2,7,18 9:4
**real**  20:7 23:10
64:22 175:18
**realistic**  182:15
**reality**  61:2 72:16
116:21
**realized**  120:22
**really**  19:2,10
21:19 30:8 74:3
98:19 105:5
106:14 111:4
115:5 116:25

136:15,23 137:3
152:3,24 167:15
**reason**  22:18 29:1
51:6 56:24 62:22
74:12 93:3 98:12
98:15 114:9 134:9
136:19 137:10,10
137:13 139:6
144:20 159:21
173:5,13
**reasonable**  56:5
164:6
**reasonably**  138:21
**reasoning**  85:22
**reasons**  74:21,25
83:19 84:9 85:4
90:19 137:12
176:5
**recall**  12:3 24:14
25:20 29:22 37:9
43:8 45:11 52:13
56:19 66:18,20
150:1
**recalling**  158:18
**receive**  24:3
119:25
**received**  24:12
48:3
**receives**  133:12
**recertification**
142:24
**recertified**  142:12
142:20
**recess**  37:4 60:5
96:4 127:6 133:1
174:23 192:23
**recipe**  143:19
**recipes**  153:9
**recognize**  24:25
182:17

J. Alex Halderman , Ph.D.
Fair Fight Action, Inc., Et Al. Vs. Raffensperger, Brad, Et Al.

[recognizing - replaced]

**recognizing** 25:1
**recollection**
189:15
**recommend** 34:16
34:17 41:23 63:19
159:25 165:24
**recommendation**
35:12,20,22 47:7
47:11,15,20,24
48:15,23,24 55:21
92:19,21 181:3
183:16
**recommendations**
47:1,25 51:12,14
56:4,8 59:11
111:10 165:13,23
188:13
**recommended**
55:13 153:24
160:8 180:6
**recommending**
35:12 55:19
133:21,23
**recommends** 47:3
47:4 48:11 49:6
51:15
**record** 56:25 57:6
57:10 59:17,19
60:2 96:2,5 97:19
107:4 110:18,23
110:24,25 111:6,7
111:14,16 161:10
161:13 192:21
**records** 38:16 66:4
111:12,13 117:6
120:24 123:13
127:23 162:4
163:20
**recount** 65:21,24
67:18 123:15
127:22 130:2

**recounts** 58:12
63:3 65:16,18,18
67:21,25 68:6
**recover** 129:24
**redacted** 44:5
**redactions** 46:13
**reduce** 87:15,17
88:20 166:1,2
**reduced** 109:24
194:11
**refer** 10:3 16:12
26:24 36:6 59:18
80:4 110:22
**reference** 30:13
42:22 54:14 59:15
66:6 113:25
120:17 139:24
149:18 188:18
189:18
**referenced** 192:15
**referred** 80:11
113:3
**referring** 16:13
26:15 45:4 55:18
63:5 70:14 121:25
126:12,16
**refers** 26:16,16
120:17
**reflect** 136:20
**reflected** 141:23
**reflects** 36:24
140:13
**regard** 45:24
**regarding** 8:24
63:14,16 178:12
178:17 188:17
**regime** 151:8
**region** 179:2
**registered** 162:5
163:20

**registrar** 104:22
105:4,6 162:8
**registrars** 162:10
**registration** 30:15
30:20 31:3,8 32:4
32:6,14,18 43:14
45:24 46:2,5
102:6,9,15 103:10
103:14 104:2,3,12
104:14,17,17,21
104:23 105:3
117:5,10,14,20
118:2,14,20 119:3
119:22 120:7,24
129:18 133:18,21
134:24 135:1
158:3 160:11,20
161:3,9,17 162:16
162:18,20,23
163:19,23
**registrations**
161:21 162:13
**regular** 120:1
126:25 127:11
**reiterating** 41:22
**reject** 86:7 89:5
**rejects** 86:12
**related** 43:6 48:23
50:11 51:19 83:5
116:7 123:25
124:6,8
**relative** 106:24
108:19 109:1
110:20 118:17
143:25 144:19
156:10 166:12,15
**relatively** 102:20
129:22 141:7
184:1
**released** 35:22

**relevant** 67:2
108:7,9 186:15
**reliable** 183:4
190:2 192:12
**reliably** 157:25
177:24 185:11
**reliance** 170:16
**relied** 13:3 164:21
**rely** 94:11 146:17
146:19 176:7
188:12 191:18
**relying** 158:7
163:4 180:19
**remain** 99:23
**remainder** 48:13
**remaining** 39:24
167:7
**remarkable** 64:3
136:15,24
**remember** 124:10
133:10
**remote** 122:3,6
**remotely** 175:19
**removable** 135:7
135:11,14,16,20
**removal** 107:25
**remove** 47:6
**removing** 108:24
**render** 47:6,20
87:11
**repair** 99:7
**repeat** 70:2 85:2
88:18 127:8
**rephrase** 7:24
62:7 170:19
186:18
**replace** 33:12 34:2
35:24 56:14 58:19
58:21 59:1
**replaced** 119:13
192:1,3

Case 1:18-cv-05391-SCJ    Document 401-1    Filed 06/27/20    Page 228 of 243
J.  Alex Halderman , Ph.D.                                   February 25, 2020
Fair Fight Action, Inc., Et Al. Vs. Raffensperger, Brad, Et Al.

[replacing - right]                                         Page 32

**replacing** 36:3 56:9
**report** 4:4,5,18 8:4 9:2,4 10:9,21 11:5 12:2,13,20,23 13:6 13:25 14:2,4,9,12 14:17,19 15:8,16 15:18 16:9 17:2 35:4,16,21 40:21 43:17,23 45:13 62:4 76:17,21,22 77:25 81:8 89:4 90:24 94:13,18,19 96:8 100:11,14 112:25 113:3 122:17 126:13 167:13,15 170:16 176:3,21 186:19 186:23 187:14 188:10,12
**reported** 66:5 67:15 170:23
**reportedly** 62:3,3 89:20
**reporter** 194:5
**reporter's** 7:6
**reporting** 43:15 62:4 186:2
**reports** 10:2 121:15 135:17 186:6,10 188:14
**republic** 68:24
**request** 7:16 33:24 69:22
**requests** 133:18
**require** 48:6 49:17 50:15 79:17 104:20 122:1 123:16,18 124:3,4 160:12 178:21 179:6 184:17

**required** 49:24 75:18,20 104:22 105:7 122:24 167:9 178:12 184:23
**requirement** 50:20 51:8 120:14 123:22 125:25
**requirements** 50:10 51:10 121:9 121:23 151:6 152:2 154:16
**requires** 50:14 123:19,20,21 150:18 163:8,11 163:14,20 184:13 184:15
**requiring** 184:19
**research** 18:11 19:6 22:23 35:5,7 35:8 42:9,16 53:7 53:9,24,25 54:8 55:13,15 60:25 72:23 80:12 126:10 172:13 175:13 177:8 180:12,19 182:12 183:20 185:13,16 185:18 187:23
**researched** 27:5,8
**researcher** 38:5
**researcher's** 187:9
**reserve** 6:15
**resiliency** 115:15
**resources** 9:1 143:22
**responsibility** 146:4
**responsible** 19:25
**responsiveness** 6:16

**result** 12:25 39:6 40:5,25 55:25 57:15,21 58:2,11 61:7 62:15 90:5 92:21 93:21 119:13 128:18 156:8 157:22 160:14 179:19 184:6
**resulted** 16:8 58:8 91:6
**resulting** 39:15
**results** 27:4 58:9 66:3,5 69:18 75:14 118:23 123:13 180:25 190:23,25 191:6 191:13,18
**retain** 21:2 69:19
**retained** 68:3,5,18 69:1
**retaining** 21:5
**return** 108:1
**returned** 108:12 108:15,18
**reveal** 40:12 66:4
**review** 8:17 9:3 11:21 69:15 70:22 92:15,24 99:2 104:23 121:13 123:5,10 126:11 136:7,9 146:10,13 147:1,20,23,24 160:2,13 164:22 171:4,5 179:20 180:14 184:12 190:8
**reviewed** 8:9,9,16 8:23 9:7 43:16,24 44:1 53:20 67:15 102:2 121:11

123:1 124:5,7 128:1 133:19 154:6,8 160:4 163:3 172:15 173:15 176:11 178:11,13 179:15 179:17 182:3 183:14 184:8 190:22
**reviewers** 152:11
**reviewing** 118:18 123:7 128:9 130:14 182:6 183:9
**reviews** 134:14
**richard** 15:24
**rid** 147:21
**rigged** 62:4
**right** 6:21 8:1 10:14 11:4 12:11 18:18 20:3,5 22:13,14,20 25:12 25:22 30:12 31:21 33:5 34:10 35:2 36:25 41:8 44:11 44:19 46:13,22 47:11,23 52:3,23 53:14 54:25 57:8 57:9,11,19,25 60:7 64:1 66:24 68:1 72:1,6,13 73:5,9 74:8 76:5,8,21 78:9,15,20,21,25 79:1,3,9 80:13 83:6,7,12 85:8,19 86:5 87:9 89:18 90:8,11,15 91:11 91:14 92:23 94:14 96:7,13 99:9 100:10 101:25 103:6 105:17

**[right - sabotaged]**

Page 33

[safe - see]    Page 34

safe  21:25 22:1
  42:15,17 155:16
  155:21 167:9
safeguard  172:10
  175:9
safeguarding
  41:23
safeguards  49:2,4
  49:5
safer  20:17,19
  42:6
sake  7:6 89:23
  90:14
samples  150:9
sampling  69:17
satisfies  48:14
saw  90:7
saying  31:11 54:1
  57:7 62:7 71:25
  75:1 78:1,2,4,5
  93:3 111:22 140:4
  141:14,16 143:12
  150:3 157:10
says  64:6 159:15
scale  148:1 186:24
scanned  48:24
scanner  69:15
  86:7,8,12 101:7,10
  107:20 138:5,6,6,8
  139:4 149:21,23
  172:18 175:5
scanners  33:13
  37:20 38:10,12,13
  38:23 39:5,8
  41:25 43:12 77:15
  77:16 78:24 79:3
  82:12 86:20 88:6
  101:2,3 122:17,23
  132:14 135:23
  138:11,12 149:19
  149:22,25 150:14

150:15 173:3,6,8
scanning  45:13
  112:14
scenario  73:21,22
  75:18 86:19
  156:16 170:3
scenarios  39:18
  54:19 77:6 78:1
  79:14,18 81:9,11
  83:24 86:10 93:21
  94:21 109:25
  117:3 126:20
  130:17,21 183:7
scenes  23:7
school  80:10
science  19:3 34:24
  48:2 93:19 94:10
  188:15
science's  181:3
  188:10
sciences  35:2,11
  180:6
scientific  89:2
  91:23 172:5 188:7
  188:17
scientifically  92:2
scientists  96:24
scj  1:7
scope  30:24
  145:23 147:16
  158:12,14,15,17
scoped  25:1
scrutiny  99:3,5
seal  175:17
seals  175:10,13,23
  175:24 176:1,5,7
  176:12,16,20
second  10:13
  30:12 32:24 33:9
  34:12 37:20 48:5
  48:18 56:9 57:17

57:18 58:15 59:16
  60:20 77:13 96:3
  103:25 105:23
  119:17 120:25
seconds  182:5
secrecy  61:22
secret  71:7,13,21
  72:10,16 99:13,19
  99:23 100:3,5,6
  151:3 152:10
secretary  1:9 6:11
  16:7 81:23 104:7
  105:24 187:21
  192:5,10
secrets  100:6
section  32:25
  58:16 76:22,24
  136:6 170:16
  174:3
sector  89:20
secure  38:25 47:2
  47:3,21 48:21
  56:3 63:20 64:12
  72:17 75:13 82:19
  83:12,16,18,21
  85:21 100:6
  138:21 139:15,17
  139:18 140:17
  145:13,16 152:19
  153:1 160:10
  174:16 191:20
securely  26:18
securing  19:15
  28:10 188:9
security  17:5,7,13
  17:17,20,24,25
  18:8 19:5,13
  22:23 23:1,22
  24:20 28:18,21
  29:4 32:17 34:1
  34:22 35:9 37:23

38:1 39:3 43:3,6
  52:24 53:14,15
  54:17,24 55:21
  60:25 64:8,23
  71:14,18,20 72:8
  74:9,16 75:2,10
  79:22 80:21,22
  81:2 83:9 84:17
  89:6 96:19,20
  98:6,11,20 99:3,11
  99:15,22,23,25
  100:18 105:1,6
  106:6 108:16
  109:25 110:2,14
  114:24 115:11,25
  116:11 118:23
  121:8,17,22 122:1
  133:22,24 139:2,3
  141:20 142:11,16
  142:21 143:1
  144:17,24 145:1,3
  145:5,7,9,11 146:5
  146:6,9,14,15,20
  147:4,9,9,14,15,24
  148:4,16,21 149:2
  151:16 152:2,16
  152:19 153:22,24
  154:4,9 155:4,7,10
  155:16 157:10
  158:13,21 159:24
  160:3 162:16
  164:13 165:12,23
  166:4,6,7 167:6
  171:4,4 174:9
  175:15,16,18,20
  176:12,18,19,23
  187:9 188:8
  190:15
see  6:23,25 8:20
  17:17 18:12,16
  25:22,22 27:21

Case 1:18-cv-05391-SCJ    Document 401-1    Filed 06/27/20    Page 231 of 243

J. Alex Halderman , Ph.D.

February 25, 2020

Fair Fight Action, Inc., Et Al. Vs. Raffensperger, Brad, Et Al.

**[see - software]**

Page 35

| | | | |
|---|---|---|---|
| 36:12 45:7,7,15 48:24 49:10 59:2 59:9 64:5,11 70:9 73:22 74:20 84:23 85:10 91:21 92:4 95:23 117:7 120:5 133:10 150:1,8 152:25 187:1 | **separate** 71:8 **september** 42:23 **sequential** 70:24 **sequentially** 70:17 **serbian** 169:13 170:20 **series** 46:13 52:12 52:13,17,19 81:9 | **ship** 141:19 **shipping** 141:18 **short** 121:7 **shorthand** 194:5 **shows** 126:10 177:8 **sign** 145:3,4,10 | **site** 23:9 **sitting** 40:7,15,23 41:15 62:14 114:6 155:24 159:22 168:20 **situation** 11:16 |

**seeing** 18:5 63:25
**seeking** 14:6
**seen** 9:24 23:15
  27:19 44:7,13
  52:18 60:14 97:9
  97:13,14 121:17
  126:1,6 135:17
  176:14
**select** 4:16,18
  37:16
**selected** 15:9
**selecting** 84:1
**selection** 87:4
  164:22 171:16
**selections** 125:7
**sell** 21:10
**senate** 4:15 30:22
  31:6 32:1,8 37:7,8
  37:16 40:20 43:16
  43:23 63:23
  113:10 134:20
**sense** 56:16 115:5
  185:10
**sensitive** 161:16
**sent** 12:4
**sentence** 7:21
  37:22 44:6 48:17
  48:18 63:13 64:6
  77:11 103:25
  104:10 105:23
  134:3 135:21
  147:8 161:14,19
  171:17

**serious** 113:13
  160:22,25
**seriously** 145:7
**served** 66:1
**server** 104:18
  150:12,19,24
  161:6 170:13
  189:25
**servers** 122:24
  123:8 189:20
  190:6
**service** 4:12 23:2
  29:21 162:1
**services** 11:11,12
  20:20 21:2,5,14
  24:1,4 51:18
  161:8 171:11
**serving** 34:6,11
**session** 25:13
**set** 50:4 56:25 57:6
  57:10 75:10 97:10
  97:13,25 98:1,22
  124:9 155:15
  167:8
**setting** 74:5
**setup** 106:7
**shape** 46:11
**share** 36:16
**shelf** 98:4,9,13,17
  141:6,13,15,16
**shield** 169:23
**shift** 122:12

**signature** 10:21
  194:23
**signed** 55:23
**significant** 17:22
  27:9 29:5 39:3
  44:25 83:7 87:24
  98:10 104:25
  106:6 112:21
  151:11 159:21
  167:16 171:3
  183:22 184:24
  185:7,10,10
  186:20
**significantly** 85:21
  118:6 152:12
  153:13 183:13
**signs** 182:10
  184:15
**similar** 37:23
  64:14 67:7 69:17
  138:2,10 148:21
  192:14
**similarly** 136:11
**simple** 55:9 71:5
  139:19,21
**simply** 51:23 52:1
  58:19 143:16
**simulated** 182:15
**simultaneous**
  179:5
**simultaneously**
  170:14
**single** 62:14

**situation** 11:16
  23:15 74:4 108:16
  110:14 111:13
  144:10 155:17
**situations** 11:15
  22:4
**six** 123:10
**size** 139:8
**skimmed** 13:15
**skip** 100:11
  179:25
**slate** 183:12
**slates** 184:2,3,4
**slower** 164:1,6
**small** 39:2 45:15
  45:18 49:16 184:1
**smaller** 33:25
  127:1,10 155:14
  186:25 187:1
**smart** 165:6,18
**social** 66:7 112:13
**software** 21:6,10
  51:16 52:25 58:18
  78:24 88:6 98:5
  98:10,23,24,25
  99:11,14 102:4,8
  102:12,15,19
  118:22 119:13,15
  119:16,20,21
  122:2 123:7 132:3
  137:16,17 138:15
  138:18,19,20
  139:8 140:1,2,10
  141:6,7,9,9,13,15
  141:17,22,22
  142:1,4,7,10,12,15

Case 1:18-cv-05391-SCJ   Document 401-1   Filed 06/27/20   Page 232 of 243
J. Alex Halderman , Ph.D.
February 25, 2020
Fair Fight Action, Inc., Et Al. Vs. Raffensperger, Brad, Et Al.

[software - states]
Page 36

142:25 143:13,13
143:17,17 144:7
144:22 145:1,12
145:13,16,16
148:15,24 149:6
149:20,21,22,25
150:20 151:12
153:4 158:12,22
158:23 169:3,17
169:21,25 170:4,6
170:7 171:9
172:14 173:11
174:8 175:2,2
177:9 179:4 180:3
188:5,20,23
189:10
**solution**  55:12,25
**solve**  72:4
**somebody**  61:17
  111:25
**somewhat**  98:8
  154:17
**soon**  132:21
  174:19 184:12
**sophisticated**
  77:12 78:9 81:5
  88:3 114:25
  116:12,22,23
  117:15 119:2
  136:14,17 143:21
  145:19 174:13
  175:6 176:4,8
**sorry**  11:1 16:23
  17:9 18:16 28:3
  45:4 50:13 59:18
  60:20 67:21 70:2
  73:7 79:21 111:17
  127:4,7 148:23
  161:18 170:18,19
  186:17 187:12

**sort**  71:6 85:16
  99:24 110:1 148:2
  189:23
**sorts**  11:22
**sos**  190:5
**sounds**  144:21
**source**  98:5,10,23
  98:25 99:14,19
  100:1,2,2 137:18
  138:6 141:13
  146:9 160:13
**sourced**  172:4
**south**  27:22 61:15
**space**  52:4 88:25
  102:17,18 119:19
**spared**  31:18
**speak**  26:3 113:9
  114:20 145:8
**speaking**  83:22
**speaks**  162:15
**special**  79:17
  113:11
**specialized**  79:12
  79:16,24 80:2
  81:8
**specific**  11:15 14:7
  62:11 63:19 73:5
  82:20 84:12 92:17
  98:19 106:21
  117:17 144:14
  149:23 153:9
  184:9
**specifically**  9:5
  35:4 43:17 75:22
  83:5,22 103:22
  118:5 121:25
  130:10 133:11
  137:20 150:12
  153:7 172:14
  173:20

**specifics**  76:20
  135:2 143:8
**speculate**  14:10
**speed**  69:15
  164:10
**spend**  23:22
**spent**  12:1 147:21
  182:5
**spike**  128:14,19
  129:16
**spoke**  9:12,12,15
**spoken**  15:16,24
  16:4,7
**sporadic**  186:10
**spotted**  162:10
**spread**  39:16,22
  46:8 135:13,19,23
  166:18 170:9,9
  190:5
**spreading**  112:12
  167:17 179:4
**staff**  43:2 51:16
**staffer**  68:15
**staffers**  37:11
**stages**  109:8
**stake**  114:10
**stamping**  48:23
**standards**  48:8
**standpoint**  34:1
  71:18,19,20 74:10
  83:21,23
**stands**  47:13
**stark**  85:13 179:13
**stark's**  179:18
**starkness**  85:16
**start**  14:22 29:19
  52:21 77:5 100:12
  107:20
**started**  7:2 12:14
  17:17 61:24

**starting**  16:25
**startup**  20:23
**state**  1:10,10 6:11
  11:22,24 13:22
  16:16,19 34:2,17
  51:19 58:21 66:23
  76:6 78:8,11,14,20
  78:25 81:3,23
  85:24 86:1 87:11
  105:24 109:23
  110:6,14 113:1,2,3
  116:15 117:10,14
  117:18 119:20
  121:9 124:5,7
  127:12 132:12,15
  135:22 139:24
  143:23 145:20
  146:17 148:4
  159:1,3,4 162:21
  175:6 178:8,11,20
  178:24 183:18,22
  184:19 187:21,24
  189:12 192:6,11
  194:2,6
**state's**  16:8 104:8
  123:1
**statement**  4:10,15
  15:1 19:11 22:7
  22:17 37:16,18
  46:14 49:11 57:19
  77:9 115:1 122:25
  125:13 136:15,24
  139:20 143:16
  152:3 154:3
  161:18,23 170:20
  171:6,15,18 176:9
**states**  1:1 30:16,17
  30:25 32:2 35:13
  35:24 36:2 46:16
  48:6 49:8,14
  51:13 58:16 59:1

Case 1:18-cv-05391-SCJ    Document 401-1    Filed 06/27/20    Page 233 of 243

J. Alex Halderman , Ph.D.

February 25, 2020

Fair Fight Action, Inc., Et Al. Vs. Raffensperger, Brad, Et Al.

[states - supposed]

Page 37

59:3,6,9 62:8 68:6
68:9,25 72:10
79:2,3,5,9,14
101:21 102:11,13
102:20,24 103:2
103:22 113:5
115:2,4,5 116:22
116:23 117:19,20
117:23 118:1,8,9
118:12 119:4,17
131:6,22,24
134:21 163:7
**statewide** 49:14,15
**statistical** 69:17
  88:11
**statistically** 88:21
  185:10
**status** 159:11
**statutory** 50:10,20
**steal** 39:17 66:8
  120:12
**stein** 66:7 68:3,5
  68:19
**stenography**
  194:12
**step** 46:22 113:8
**steps** 23:6 116:20
  159:4,12 160:3
  163:15
**stick** 67:18 107:19
**stolen** 40:24 61:1,3
  61:4 62:9
**stood** 186:12
**stop** 138:22
**stopped** 41:10
**stopping** 41:3
  76:14 94:17
**store** 97:20
**stories** 29:8
**story** 4:20 52:10

**straight** 56:25
  57:6,10
**straightforward**
  55:10
**street** 2:4 45:14
**stretch** 33:6
**strike** 40:22 68:20
  111:21,23 112:18
  153:9
**stringent** 153:21
  154:4,16 155:3
**strong** 42:16 64:23
  92:9 110:9 122:25
  175:15 177:5
  181:7
**stronger** 96:18,20
  143:16
**strongest** 55:21
**strongly** 42:20
  110:3,18 122:10
  140:12
**structure** 168:5
**struggling** 35:25
**student** 183:2,3,5
**students** 19:24
**studied** 117:21
  118:10,12,13
**studies** 92:12,15
  92:16 126:12,15
  126:16 180:20
  181:2,9
**study** 5:15 17:15
  82:23 93:17 94:7
  139:14 156:4
  171:25 177:14
  180:13 181:11,13
  182:3,4,5,9,13,25
  184:8 185:2,6
  186:9
**studying** 17:15,17
  60:24 79:22 184:9

**stuff** 170:12
**stuxnet** 135:8,13
  135:15,18
**style** 125:16
  172:25
**subcommittee**
  4:11 29:20
**subhead** 60:23
**subject** 78:8 88:3
  89:16 90:9 122:6
  165:1 166:3,3,6,7
  177:17
**subparagraphs**
  117:2
**subpoena** 12:25
  13:2
**subsequent** 30:21
  35:7 180:12,19
  188:14,24
**subset** 28:9 59:22
  184:3
**substantial** 33:22
  35:7 40:4 58:10
  62:12 66:14 90:22
  91:3 159:15 181:5
**substantially**
  109:24
**substitute** 123:7
**subvert** 117:4
**succeed** 65:18
  77:17 79:8 115:9
  127:19 140:6
**successful** 40:14
  113:1
**successfully** 31:16
  45:19 61:8,9,18
  83:10 137:8
  143:21 169:10
**suffer** 37:22
  154:20

**sufficient** 51:25
  125:15 126:17
  128:1,9 129:3
  130:14 152:16,19
  156:25 159:13
  161:25 167:20,23
  172:10 178:8,21
  179:7,21
**sufficiently** 53:20
  115:18 128:8
  129:1 130:1,4,9,15
  136:14,17 153:1
  153:11 155:13
  173:22 174:1
**suggest** 153:8
**suggested** 187:23
**suggestive** 180:23
**suite** 2:12 101:13
**summarize** 77:2
**summarizes** 76:23
**summary** 77:23
  114:21
**superior** 36:19
  85:23 86:4
**supplement** 4:5
**suppliers** 169:4
**supply** 169:1
  171:25 172:1
**support** 64:12
  73:15,24 74:3
  124:15,17
**supported** 42:16
  59:5
**suppose** 12:15
  17:19 24:10 28:23
  51:3 57:14 63:18
  89:9 137:15 148:8
  148:11 163:22
  164:16
**supposed** 12:19

**[sure - takes]**                                                    Page 38

| | | | |
|---|---|---|---|
| **sure**  13:16 17:13 | 72:25 73:11,12 | 147:22 149:3,7,16 | 104:13,18 116:18 |
| 18:7 22:23 23:23 | 74:24 75:5,16 | 152:13,15,23 | 122:17 126:9 |
| 27:19 29:8 33:3,7 | 76:7 77:7,14,22 | 153:2,7,10,14,15 | 131:23 133:8 |
| 46:4 47:10,23 | 78:7,10,13,19,25 | 153:19 154:9,12 | 134:21 135:19 |
| 48:12 59:5 65:7 | 79:12,15 80:5,8,19 | 154:25 155:15,20 | 136:11 137:5,8,18 |
| 70:3 72:19 76:24 | 81:1,6,16,17,20,20 | 156:1,21,23 | 137:19,20,23 |
| 82:22 85:3 89:15 | 81:21 82:9,10,13 | 160:20 161:5,16 | 138:1 139:5,19,21 |
| 94:5 95:8 104:4 | 82:16,17,18,19 | 161:22 162:7,17 | 144:12,14 147:11 |
| 104:20,25 106:2,9 | 83:2,8,12,20 84:1 | 162:19,20,23 | 153:1 159:20 |
| 106:11,11 107:24 | 84:18 85:8,14,15 | 164:19 165:19 | 167:17 175:14 |
| 108:4 111:1 116:3 | 85:19,20 86:9 | 166:19 167:22 | 180:23 181:1,7 |
| 118:5 127:5,10,18 | 87:4,9,20,25 88:2 | 168:5 169:23 | 189:13 |
| 131:6 137:6,19 | 88:4,5,9,25 89:8 | 170:10,12,25 | **sytem**   100:2,3 |
| 140:13,23 141:10 | 89:23 91:1,2,18,19 | 171:10 172:20,21 | |
| 141:17 148:12 | 92:8 93:10,12,25 | 172:23 179:5 | **t** |
| 150:6 152:7 160:1 | 94:24 95:6 97:18 | 180:4,5 187:2,24 | **tabulated**  61:15 |
| 162:9 168:2 169:9 | 99:21 100:1,6,19 | 190:5,21 191:11 | 82:12 |
| 170:24 174:5,7,20 | 100:20,21,22 | 191:23,25 192:2,4 | **tabulating**   62:23 |
| 181:23 | 101:13,24 103:1,5 | 192:16,17 | **tabulation**   73:3 |
| **surefire**   128:3 | 103:10 105:1 | **system's**  82:2 | **tabulators**   63:15 |
| **surprise**   65:4,6,7 | 106:4,25 107:7 | **systematic**   66:5 | 63:17 |
| **surrounding** | 108:20 109:19 | 156:25 | **take**   7:15 33:3,5 |
| 121:10 | 110:2,7,8,20 | **systematically** | 36:14 37:1 41:2 |
| **susceptible**   138:17 | 112:15 114:1 | 57:23 | 58:20 75:9 90:25 |
| 187:25 | 116:15 117:16 | **systemic**   156:7 | 107:9 116:20 |
| **swore**   61:22 | 119:13,15,16 | **systems**   5:14 | 132:21,22 145:6 |
| **sworn**   6:6 194:9 | 121:10,20,21 | 15:22 19:4 20:9 | 156:12 157:11 |
| **system**   8:14 20:4,6 | 122:3,6,14,19,20 | 20:25 22:2 30:15 | 166:9 173:7 |
| 20:11,12 21:24 | 122:21,22 123:2 | 33:12,13,16 39:23 | 174:19,20 185:25 |
| 23:17,20 26:14 | 124:1,2 125:2 | 44:16 45:16 46:2 | 186:3,8,13 |
| 29:2,3,6 30:20 | 126:4,5,8 131:18 | 46:3,5,8 53:12 | **taken**   1:18 6:10 |
| 31:3,4,7,8,10 32:6 | 132:15,16 133:4,9 | 54:18 56:3,10 | 7:3 13:10 37:4 |
| 32:14,18 33:18 | 133:14,16,17 | 58:3 59:15 60:4 | 42:10 60:5 91:24 |
| 34:2,3,8,9 38:20 | 134:2,14,17,24 | 62:16,19 63:6,20 | 93:4 96:4 127:6 |
| 38:23 39:3 42:12 | 135:1 136:1,2,4 | 70:21,25 72:18 | 133:1,24 159:4,12 |
| 45:24 47:16,17,19 | 137:4,7,22,25 | 74:21 79:23 81:23 | 162:11 163:15 |
| 47:21,24 48:9,10 | 139:6,15,16,18,22 | 82:1,6 83:13 85:5 | 167:19 172:10 |
| 49:1 51:4 54:2 | 140:8,18,19 | 87:13 90:4 92:8 | 174:23 192:23 |
| 55:11 56:13 59:16 | 141:24,25 142:3 | 93:1 97:2 98:6 | 194:8 |
| 62:4 65:2 67:14 | 142:15 143:11,22 | 101:17,19,20 | **takes**   157:13,16 |
| 69:14,25 72:23,24 | 146:8,10,12 147:2 | 103:9,13 104:11 | 187:5 |

**[talk - think]**                                                          Page 39

**talk** 7:7 8:2 9:10
  12:11 16:24 28:4
  29:18 37:6,19
  52:5 76:16,18
  80:16 84:11
  104:10 113:22
  122:16 125:5
  133:3 135:5 136:4
  141:5 158:4
  160:19 169:11
  175:9
**talked** 9:18 28:6
  38:3 53:22 65:10
  86:10,14 88:2
  111:24 114:14
  125:24 179:22
  189:20
**talking** 23:10 47:8
  48:14 81:4 88:19
  169:5 173:20
**talks** 63:22 144:17
  149:5
**tamper** 175:10,13
  175:17
**tampering** 43:11
  173:10
**target** 114:5,8
  122:10 140:5
**targeted** 14:7
  30:20 31:10 46:16
  77:8,12 88:3
  89:17 113:5
  134:17,22,24
  135:6
**targeting** 30:14
  31:9,22 46:20
  78:8 90:10 113:6
**taught** 19:8
**tautologically**
  142:3 150:16

**taylor** 2:11
**taylorenglish.com**
  2:15
**teach** 80:15
  191:20
**teaching** 19:7
  138:22
**tech** 15:24,25
**technical** 11:18,21
  17:21,22,25 32:3
  41:3 64:22 117:17
  136:7 159:13
  163:5 172:15
**technically** 92:16
**techniques** 84:16
**technological** 72:7
**technologies** 27:2
**technology** 19:15
  24:18 26:17,23
  39:22 72:13 82:15
  114:23 115:2,4
  116:8,17 117:4
  118:14 140:20,21
  140:22,25 164:7,9
**tell** 17:8 22:22
  26:4 51:22 52:19
  52:21 82:25 124:9
  143:24 144:6,15
  147:7 164:17
  191:8
**ten** 33:3 137:24
  185:1
**tend** 148:15
**tends** 141:10
**tenured** 18:19
**term** 143:5
**terminology**
  111:11
**terms** 8:16 19:7,21
  26:13 29:1 44:10
  45:22 49:13 59:11

63:2 67:13 87:12
  94:20 111:1
  112:17 131:11
  144:15 165:1,3,22
  167:9,15 183:16
  184:21 185:11
  186:24
**terrible** 170:12
**test** 146:22 150:7
  177:9,17
**tested** 98:18 101:3
  101:6,9,12,15
  173:2 188:19,23
**testers** 149:12,14
**testified** 6:7 29:20
  45:3
**testify** 37:12 194:9
**testifying** 40:20
  63:23 192:16
**testimony** 16:10
  16:18 29:18,19,22
  30:3,19,21,22 31:2
  32:5,8 37:7 41:5
  41:24 42:4 44:18
  44:21,23,24 47:14
  48:4 63:7,12
  83:11 103:4 105:5
  106:13 110:5
  122:5 125:15
  131:19 135:10
  137:21 140:16
  145:12,15,18
  146:17 159:17
  162:6 169:12
  170:11 175:3,16
  190:18,20,25
  194:11,15
**testing** 8:21 146:9
  146:15 147:5,9,9
  147:14,15,24
  148:4,21 158:13

164:14,17 177:1,5
  177:19,21,24
**tests** 101:21,23
  147:5 150:13
**texas** 8:25
**text** 125:10 126:8
**thank** 54:12
  111:19 132:25
  187:4,20 193:2,4
**theory** 61:1
**thesis** 17:4,10
**thing** 42:6 59:2
  61:21 72:3 96:9
  110:1 126:19
  135:4 155:9
  179:23
**things** 22:9 31:24
  51:18 53:24 64:12
  76:16 77:2,19
  78:11 81:10 90:1
  93:15 100:7
  110:19 111:4
  114:5 118:21
  129:22 132:14
  135:13 140:11
  149:7 153:4,6
  159:15 160:13
  179:23 182:10
  186:11 190:16
**think** 5:10 8:25
  11:16 15:3,5
  16:15 22:1,8 25:1
  28:18 31:5 32:11
  32:16,19,25 33:1
  38:3 39:24 40:4
  42:5,13,17,18
  47:12,18,19 49:5
  57:25 58:1,10,25
  59:11,25 60:21
  61:6 62:11 64:11
  65:5 66:12 70:8

J.  Alex Halderman , Ph.D.

February 25, 2020

Fair Fight Action, Inc., Et Al. Vs. Raffensperger, Brad, Et Al.

**[think - trying]**

Page 40

| | | | |
|---|---|---|---|
| 71:2 74:9,11,22 | **threat**  79:25 119:2 | 193:2 | 107:1,3,8,9,12 |
| 75:17 76:6 77:20 | 190:13 | **told**  86:15,16,17 | 109:6 |
| 77:22 79:24 80:3 | **threats**  43:10,10 | 86:19 125:24 | **transmit**  105:24 |
| 83:16 84:3,19 | 169:1 | **tongue**  120:21 | **transported**  29:10 |
| 88:2 89:10,25 | **three**  30:13 33:9 | **top**  18:16 39:11 | **travel**  24:3 |
| 91:12,21 92:5,5 | 49:17 68:8,9 | 45:6,9 55:9 69:24 | **trench**  66:17 |
| 93:23 94:1,2,16 | 69:24 138:14 | 77:3 92:15,24 | **trial**  6:16 |
| 97:4,14 98:7 | **threshold**  92:1 | 94:3 144:14 | **tricky**  22:7 |
| 99:10 103:16 | 93:17,20 | 147:20 150:2 | **tried**  43:1 71:2 |
| 104:7 105:9,22 | **throw**  127:14 | 182:8 | 109:2 149:10 |
| 107:3,11,17 108:3 | **thrown**  29:9 | **topic**  17:9,11 | 150:8 |
| 109:15,21,24 | 111:11 | 24:19 26:19 54:4 | **tries**  93:8 |
| 110:19 111:17 | **tie**  70:18 | 54:20 185:16 | **trigger**  31:20 41:7 |
| 112:16,18 113:16 | **time**  12:1,3 18:4 | **topics**  19:23 26:5 | 41:9 114:15,18 |
| 115:3 122:22 | 18:10 23:23 36:14 | 43:6,7,8 | **trisha**  1:22 194:5 |
| 123:11 128:11,23 | 42:1,5,18 48:20,23 | **total**  39:4 | 194:24 |
| 129:2 134:22 | 54:21 57:25 59:20 | **totally**  7:22 11:2 | **trivial**  22:2 |
| 135:17 136:6,18 | 61:17,23 62:6 | 91:22 | **true**  28:17 34:8 |
| 141:2 145:3 | 70:16 75:9 121:7 | **totenberg**  67:6 | 38:3 47:15,16 |
| 146:19 151:10 | 141:18,20 142:10 | **totenberg's**  9:9 | 48:8,10 61:6 |
| 152:7 154:15,21 | 148:1 157:23 | **touch**  29:3 54:20 | 72:15 115:1,3 |
| 154:22,25 155:11 | 166:9 179:8 193:2 | **touches**  53:9 | 117:13,16 125:2 |
| 155:21 159:20 | **timeline**  11:19 | 177:17 | 129:2 131:16 |
| 160:12,21 162:15 | **times**  4:20 7:19 | **track**  170:12 | 132:12,17 137:11 |
| 164:5 166:9 167:6 | 52:6,10,14 53:2 | **trade**  72:3 89:6 | 137:13 138:17 |
| 171:12,15 175:1 | 54:22 70:19 | 99:13,19 | 139:10 148:24 |
| 177:17 179:21 | 137:24 185:1 | **trail**  36:23 47:5 | 152:20 153:4,6,14 |
| 188:4 191:3,4,19 | **timing**  18:2 | 53:17 115:7 128:5 | 170:7,14 171:9,15 |
| **thinking**  73:23 | 178:19 | 136:20,20,21 | 172:20 176:16 |
| 74:1 76:13 90:23 | **tipping**  92:2,4,5 | 140:12,13 | 178:1,5 194:14 |
| **third**  25:8 37:21 | **titled**  17:5 52:10 | **trails**  36:7 | **trump**  68:10 |
| 38:18 41:11 48:11 | 60:20 | **training**  79:17 | **trust**  38:8 140:22 |
| 48:21 59:13 63:21 | **today**  7:2 8:3,8,9 | **transcribed** | **trusted**  23:8 |
| 64:1 65:16 77:14 | 8:18 9:4,6,11,18 | 194:13 | **truth**  194:9,10,10 |
| 134:3 | 27:6,7,10 40:7,15 | **transcript**  7:14 | **try**  116:20 127:2 |
| **thoroughly**  109:16 | 40:24 41:15 42:9 | 194:15 | 127:14 129:15 |
| **thought**  16:20 | 58:7 62:14 119:15 | **transcription** | 149:11 177:16 |
| 53:25 56:4 57:14 | 121:22 138:25 | 194:14 | 191:17 |
| 71:2 80:22 | 141:9 153:3 | **transferring**  159:1 | **trying**  20:13 23:19 |
| **thousand**  8:12 | 157:20 159:5,10 | **transmission** | 23:23 58:22 66:8 |
| | 159:22 168:20 | 106:1,5,14,21,23 | 74:13 82:2 84:7 |

Case 1:18-cv-05391-SCJ    Document 401-1    Filed 06/27/20    Page 237 of 243
J.  Alex Halderman , Ph.D.    February 25, 2020
Fair Fight Action, Inc., Et Al. Vs. Raffensperger, Brad, Et Al.

[trying - use]    Page 41

85:3,11 88:7 89:1
93:9 95:19 143:10
152:22 156:15
192:13
**ts**  66:22 67:10
95:12
**tsx**  67:10 95:13
**tuesday**  1:21 6:2
**turn**  25:8 37:19
39:11 44:3 45:2
51:12 55:8 57:18
58:14 62:20 69:23
96:8 100:10 127:4
**turning**  133:3
**turns**  84:18
**twister**  120:21
**two**  15:25 16:2
31:23 39:19 49:17
59:14 63:21 69:24
70:22 71:8 115:14
125:8 126:12,16
148:14 158:5
180:20 181:9
**type**  22:25 67:8
73:19 95:20
120:25 125:1
129:23 152:4
162:6,12
**types**  17:14 53:23
82:1 87:19 106:14
106:18 125:8
130:19 132:14
160:17
**typical**  23:19
**tyson**  2:10 3:5 6:9
6:20,23 9:21 10:8
10:14,17 11:2,3
25:4 27:14 30:1
30:11 37:5,14
43:22 45:8 52:8
55:4 56:23 60:6

60:10 69:9 70:6
96:5,6 97:8 107:5
127:9 133:2
174:24 182:24
192:21,24 193:1

**u**

**uh**  7:13,13 176:17
**ukrain's**  113:24
**ukraine**  62:2
**ukrainian**  113:23
**ultimate**  90:24
**ultimately**  22:16
29:2 53:10 88:14
140:7 148:3 152:1
152:20 153:18
155:6 164:8 185:6
**un**  61:16
**unacceptable**
92:20 157:5
167:21 168:3,10
168:14,22
**unauthorized**
161:14
**unaware**  176:24
**unclear**  146:7
**uncovered**  74:23
**underestimated**
10:25
**undergrad**  17:18
**undergrads**
138:23
**undergraduate**
16:25 17:4
**underlie**  87:4
**underneath**  57:17
**understand**  7:25
20:24 21:7,11,21
47:14 85:3,11
88:7 125:19
133:16,19 143:18
147:25 152:22

156:15 162:25
163:11 184:11
**understanding**
35:9 46:17 51:8
51:11,18,21
100:21,23 101:24
104:8 105:18,20
107:23 123:17,19
124:2 125:25
133:8 155:18
159:8 162:18,22
165:7,21 178:13
178:24
**understands**  21:13
**undertaken**  123:9
**undertook**  68:12
**undesirable**  91:6
**undetected**  83:4
125:12 126:18
**unencrypted**
151:14,15
**unfortunate**
191:10
**unfortunately**
41:17 79:5 90:4
110:9 115:22
116:21 146:16
148:20 157:16
178:5
**unique**  173:12
**united**  1:1 62:8
68:25 72:10
131:22,24
**universal**  153:12
**university**  5:15
9:14 18:14,15,19
18:23 21:23
189:12
**unmistakable**
186:13

**unpatched**  144:9
**unredacted**  44:6
**unrelated**  87:5
**unsigned**  10:13
**unsuccessful**
61:11
**unsuccessfully**
45:16
**untraceable**  67:12
**unwise**  141:2
**update**  104:12,13
133:13 142:11
159:11,13 162:1
**updated**  104:15,16
104:21 162:7
**updates**  141:20
142:17
**updating**  51:16
**uploaded**  104:18
**urge**  173:13
**usability**  25:13
26:4,9,12,14
**usb**  107:19 151:2
**use**  6:17 26:17,23
27:2 35:13 42:6
46:1,4 58:16
59:14 69:19 71:6
73:15 79:2,3
82:20 84:16 89:13
89:22 90:13 91:10
92:2 97:18 98:4
102:11 104:1,2
105:15,20 111:3
116:19 119:15
121:6 122:15
127:2 128:13
132:6 140:20
141:10,12,14,16
143:25 145:24
153:12 154:19,24
156:5 162:3 164:7

**[use - voters]**                                                                Page 42

165:25 168:21
173:18 176:5,12
177:15 182:9
184:2,3,4 185:22
**users** 26:21
**uses** 33:19 81:17
81:21 155:2
**usually** 107:23
126:22 187:8
**utilize** 38:24 39:1
153:23

**v**

**vacant** 144:18
145:8
**valid** 97:23
**validation** 35:5
**valuable** 191:19
**value** 93:22,22
174:8,9 175:24
176:1 191:16
**variabilities** 50:6
**variation** 129:19
**variations** 129:20
**variety** 77:6
**various** 29:10
54:19 100:25
114:5 179:22
183:7 190:16
**vast** 184:4
**vector** 87:8,10
**vectors** 80:3 82:7
82:8 87:12
**vendor** 46:8
119:19 159:23
160:9
**vendors** 39:22
51:17 119:3 160:5
**verbal** 182:10
183:8,11,25
184:14,18,20
185:2,5

**verifiability**
157:22
**verifiable** 26:11
27:1 36:7,23
110:24 111:5,6,11
**verification** 24:13
24:16,17 25:14
26:5 35:6 83:8
157:12 180:20
184:10,21
**verified** 5:12 47:5
96:12,15,17,17
97:2,21 110:18,22
110:24 111:5,7,8
124:11 156:19
**verify** 38:15 83:10
111:7 129:4
157:25 181:12
182:11
**verifying** 83:5
110:10,11 111:12
128:25,25 156:18
157:23 183:18
**versa** 103:10
**version** 10:13
97:14 102:23
103:20 141:18,19
142:6,7,16 144:1
146:22,23,24
188:20,24,24,25
189:9
**versions** 102:13,19
102:23 103:21
144:4 146:12
148:15,15
**versus** 16:19 65:1
65:15 81:16,21
83:1 85:5 87:18
98:14,23 99:14
102:23 103:21
129:13 164:4

171:21 174:8
177:18 186:25
**viable** 190:13
**vice** 103:10
**victory** 186:15,20
186:22,25,25
187:1
**video** 52:6,11,13
52:19,22,23 53:3,6
54:22 67:2,12
**videos** 52:16,18
**view** 42:8,13 57:14
65:22 104:12
185:21
**views** 66:13,14
91:13,15,16
101:17
**vigo** 111:24
**violated** 13:22
**viral** 188:23
**virtue** 20:11
**virus** 126:2,7
135:8 188:18,19
**visibility** 24:7
112:22
**visible** 191:9
**visited** 121:12,16
**visiting** 112:13
**vladimir** 41:8
**vote** 5:9 47:2
60:20 62:23 63:15
63:17 71:16 90:21
105:16,19 112:7
113:24 131:7
177:11 188:9
**voted** 111:18
**voter** 25:13 26:5
30:15,20 31:3
32:3,6,14,18 35:5
36:7 45:24 46:2,5
47:5 60:4 70:17

83:8 85:25 86:11
97:20 102:6,9,15
103:10,13 104:1,3
104:12,14,15,16
104:16,17,21,22
104:23 105:3
110:18,22,24,24
111:6,7,7,8,11
117:5,10,14,20
118:1,13,19 119:3
119:18,22 120:17
120:23 129:17
133:18,21 140:13
141:1 157:9,11
158:3 160:10,20
161:3,9,16,21,24
161:25 162:1,16
162:18,20,23
163:18,23 165:20
177:10,10 180:20
184:9
**voter's** 125:6
**voters** 5:16 13:23
26:21 33:20,23,24
33:25 36:24 38:17
42:2,7,12 59:23
61:19 70:19 73:14
73:24 74:6 79:2
81:19 82:11,17,25
83:5,9 86:22
91:20 104:11,13
105:11,15,19
110:10 111:12
119:24 120:13
126:10 128:1,8,24
129:4 130:14
134:9 136:21
140:12 153:13,15
154:19,24 155:3,9
155:11,14,18
156:3,6,16,18,19

Case 1:18-cv-05391-SCJ   Document 401-1   Filed 06/27/20   Page 239 of 243
J. Alex Halderman , Ph.D.                              February 25, 2020
Fair Fight Action, Inc., Et Al. Vs. Raffensperger, Brad, Et Al.

[voters - wireless]                                          Page 43

156:23 157:15,23
157:25 161:10
162:4 163:21
177:17 179:7
180:10,14 181:12
182:5,10 183:9,13
183:18 184:3,5,14
185:8,19 186:1,23
**votes** 39:17 40:24
44:7,18 53:1
61:15,19 64:24
65:4,5 70:16
71:23 91:7 97:21
105:12 112:12,19
113:11,15,17,20
177:18
**voting** 5:12,13
15:9,10 18:4,9
26:11 27:1 33:12
33:20 36:3 37:21
39:14 40:25 43:11
44:8,21,23 47:4,16
47:17,18,21 52:12
52:24,25 53:12,16
54:8 56:3,9 60:25
61:5 62:9,16,18,23
63:4,5,14,17 66:18
66:20 67:13 70:19
70:25 73:10,25
76:8 79:23 82:6
83:12,13 92:8
94:25 95:6,8,12
96:13,15,17,17
97:2,3,21,23 98:6
99:13 100:21
101:19 107:21
110:7 114:23
115:2,4 116:18
120:15 124:12
131:15,18 134:10
136:11 137:4,7,19

137:23,25 140:17
140:20 142:14
163:12,25 166:19
175:25 176:16
178:9,22 181:21
181:23,24 191:5
**vouched** 23:8
**vouches** 23:4
**vs** 1:7
**vulnerabilities**
20:1,2,9,22,25
21:20,24 22:3,6,9
22:12,15 24:8
38:1,19 43:5
45:13 80:8 88:9
92:17 99:6 103:1
112:14 116:8
119:6 139:10,12
139:25 140:3
143:2,3,12,14,19
144:6,10,12,13
147:7,10,11,13
148:16,19,25
149:3 152:21
157:11 159:18,19
160:23,25 161:1
161:15 189:19
**vulnerability**
24:11 38:5 90:19
143:4,4,5 144:9
168:16
**vulnerable** 33:12
35:24 58:23 118:3
118:7,10 138:18
144:6,23 180:2
192:18
**vvpat** 60:4
**vvpats** 36:7,15,18
180:23,25 181:2
**vvsg** 48:8

**w**

**wait** 7:11 30:10
97:10 128:16
**walk** 17:2 44:2
100:13,25 146:21
**walking** 45:14
**want** 5:5 7:1,15
8:1 17:2,12 20:21
22:12 33:3 37:6
44:2 49:16,19
52:3 57:18 69:7
76:16,17 77:2
110:21 116:25
134:9 168:2
181:10 191:2,3
**wanted** 56:25 57:6
96:9 97:17 100:13
109:16
**wanting** 17:15
**wants** 51:4 148:4
**washington** 2:5
5:1 54:23 55:5
67:5
**way** 7:16 10:2
20:1,12 29:4
31:14 40:10,13
41:20 42:4,20
46:25 50:7 51:22
53:1 65:8 67:10
67:16 71:2 75:12
84:8,25 86:21
87:2 94:22 97:23
109:5 125:7
126:22 127:24,25
128:3,6,21 129:15
132:10 133:13
135:18 140:4,17
154:25 155:25
156:9,9,13 157:25
163:25 169:15
173:4 183:17

186:12 190:2,2
191:9,10 192:12
192:13
**ways** 20:14 84:14
105:3 135:7
140:21 177:15
**we've** 9:22 10:5
25:5 28:6 30:2
37:15 43:20 46:20
49:6 52:9 55:1
57:1 60:8 69:7
79:8 80:11 90:13
102:1 109:15
133:7 136:6,16
146:25 160:20
175:1 179:21,23
182:22 188:1,14
**weakness** 70:13
**weaknesses** 37:23
**website** 4:6,7 23:5
23:10 25:7 27:15
97:15 160:23
**websites** 23:5,14
112:13 161:1
**week** 23:13
**weeks** 122:15
**weigh** 85:3
**welcome** 185:16
**wenke** 15:25
**went** 8:20 178:2
**whatsoever** 38:24
**wick** 1:18
**widely** 102:12,16
169:25 170:4,6,7
**wifi** 163:13
**wild** 72:14,15
**willing** 57:8 73:24
88:15 104:9
**winner** 126:18
**wireless** 47:6
163:8

J. Alex Halderman , Ph.D.
February 25, 2020
Fair Fight Action, Inc., Et Al. Vs. Raffensperger, Brad, Et Al.

**[wisconsin - zero]**
Page 44

Georgia Code

Title 9, Chapter 11

Article 5, Section 9-11-30

(e) Review by witness; changes; signing.

If requested by the deponent or a party before

completion of the deposition, the deponent shall

have 30 days after being notified by the officer

that the transcript or recording is available in

which to review the transcript or recording and, if

there are changes in form or substance, to sign a

statement reciting such changes and the reasons

given by the deponent for making them. The officer

shall indicate in the certificate prescribed by

paragraph (1) of subsection (f) of this Code

section whether any review was requested and, if

so, shall append any changes made by the deponent

during the period allowed. If the deposition is not

reviewed and signed by the witness within 30 days

of its submission to him or her, the officer shall

sign it and state on the record that the deposition

was not reviewed and signed by the deponent within

30 days. The deposition may then be used as fully

as though signed unless, on a motion to suppress

under paragraph (4) of subsection (d) of Code

Section 9-11-32, the court holds that the reasons given for the refusal to sign require rejection of the deposition in whole or in part.

DISCLAIMER:  THE FOREGOING CIVIL PROCEDURE RULES ARE PROVIDED FOR INFORMATIONAL PURPOSES ONLY. THE ABOVE RULES ARE CURRENT AS OF APRIL 1, 2019.  PLEASE REFER TO THE APPLICABLE STATE RULES OF CIVIL PROCEDURE FOR UP-TO-DATE INFORMATION.

VERITEXT LEGAL SOLUTIONS
COMPANY CERTIFICATE AND DISCLOSURE STATEMENT

Veritext Legal Solutions represents that the
foregoing transcript is a true, correct and complete
transcript of the colloquies, questions and answers
as submitted by the court reporter. Veritext Legal
Solutions further represents that the attached
exhibits, if any, are true, correct and complete
documents as submitted by the court reporter and/or
attorneys in relation to this deposition and that
the documents were processed in accordance with
our litigation support and production standards.

Veritext Legal Solutions is committed to maintaining
the confidentiality of client and witness information,
in accordance with the regulations promulgated under
the Health Insurance Portability and Accountability
Act (HIPAA), as amended with respect to protected
health information and the Gramm-Leach-Bliley Act, as
amended, with respect to Personally Identifiable
Information (PII). Physical transcripts and exhibits
are managed under strict facility and personnel access
controls. Electronic files of documents are stored
in encrypted form and are transmitted in an encrypted
fashion to authenticated parties who are permitted to
access the material. Our data is hosted in a Tier 4
SSAE 16 certified facility.

Veritext Legal Solutions complies with all federal and
State regulations with respect to the provision of
court reporting services, and maintains its neutrality
and independence regardless of relationship or the
financial outcome of any litigation. Veritext requires
adherence to the foregoing professional and ethical
standards from all of its subcontractors in their
independent contractor agreements.

Inquiries about Veritext Legal Solutions'
confidentiality and security policies and practices
should be directed to Veritext's Client Services
Associates indicated on the cover of this document or
at www.veritext.com.